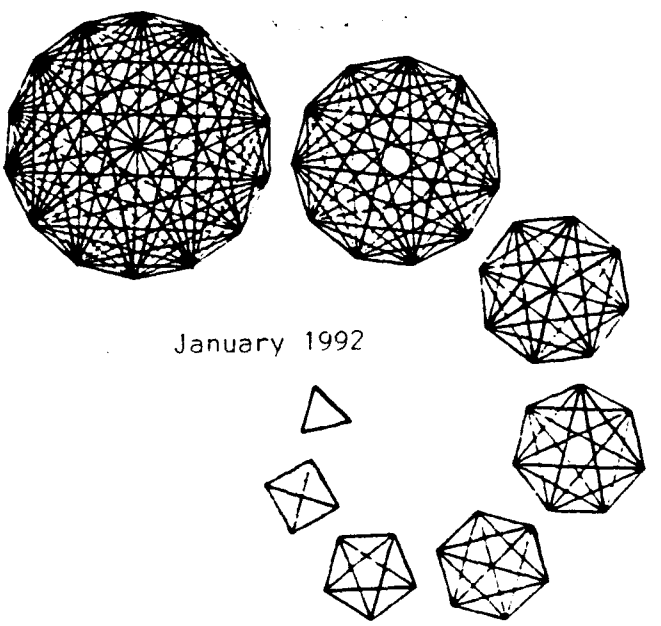
CENTER FOR PURE AND APPLIED MATHEMATICS
UNIVERSITY OF CALIFORNIA, BERKELEY

PAM-545

ANALYSIS OF PROJECTIONS OF THE TRANSFER MATRIX IN 2D ISING MODELS

Wee-Liang Heng



January 1992

This report was done with support from the Center for Pure and Applied Mathematics. Any conclusions or opinions expressed in this report represent solely those of the author(s) and not necessarily those of the Center for Pure and Applied Mathematics or the Department of Mathematics.

Analysis of Projections of the Transfer Matrix in 2D Ising Models*

by

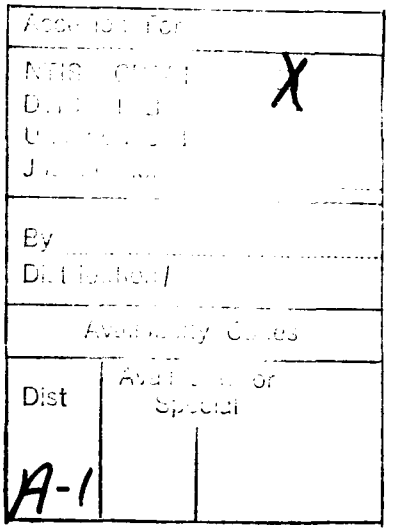
Wee-Liang Heng

Abstract

The Ising model, originally proposed to explain properties of ferromagnets, consists of a regular lattice whose vertices are considered to be 'sites' that can be in exactly one of two possible states. Of interest is the partition function, which is the sum of the energy of the lattice over all possible configurations. There are two main approaches to computing the partition function: the combinatorial method uses an expansion whose coefficients are the number of subgraphs satsifying certain criteria; the algebraic approach introduces a transfer matrix whose spectral radius is the partition function per spin. In the semi-infinite 2D model with n rows, the associated transfer matrix M_n is duodiagonal of order 2^n. This thesis introduces a special class of subspaces for approximating the dominant eigenvectors of M_n, and analyzes the projections of M_n and its adjoint onto these subspaces. We shall show that the projections are sparse (with 2 or 4 nonzero entries per column), and are of order $O(n^2 2^{l-1})$ where l is a parameter of the subspaces. Some optimal properties of these subspaces are established.

*The author gratefully acknowledges partial support from ONR contact No. N00014-90-J-1372.

Contents



Chapter 1

Introduction

1.1 Summary

The Ising model was proposed to explain properties of ferromagnets but since then it has found application to topics in Chemistry and Biology as well as in Physics. The model arose in Statistical Mechanics and consists of a regular grid whose vertices are considered to be 'sites' that can be in exactly one of two possible states. In the original version [Isi25] each site held an orientable particle that could have its spin μ parallel to an external magnetic field ($\mu = +1$) or antiparallel ($\mu = -1$) to it. Another application (the formation of binary alloys) has $\mu = +1$ if the site contains an atom of type A and $\mu = -1$ if it contains an atom of type B. In studying gases $\mu = +1$ if a site is occupied by a molecule or $\mu = 0$ if it is empty. An excellent introduction to the Ising model targeted at a general audience is [Cip87].

Early work focussed on 1D lattices but the subject really came to life in 1944 when Onsager [Ons44] derived an exact closed form expression for the partition function (see below) for an infinite 2D grid with no external magnetic field. This expression exhibited the desired singularity that signals a critical temperature T_c at which a phase transition occurs. Specifically the residual magnetization $M_0(T)$ that remains when the external magnetic field is turned off is positive and decreases steadily to zero as $T \to T_c$ from below but simply vanishes for all $T \geq T_c$.

Exact solutions for nonzero magnetic fields have not been found so far and a number of researchers have turned to approximations. There are two main approaches.

The combinatorial method uses an expansion of Z_N, the partition function for N

sites, that involves for its r^{th} term the total number of subgraphs in an N-node graph with exactly r edges subject to certain constraints. Considerable effort has gone into counting these graphs but we shall say no more on this topic. See [Kac68] for further discussion.

The algebraic, or matrix method is based on the creation of a *transfer* matrix whose spectral radius (the largest magnitude among the eigenvalues) yields the partition function per spin [KW41]. This study is concerned with projecting the transfer matrix onto a class of special subspaces but first we introduce the partition function and the related transfer matrix.

Suppose that the grid contains N sites and is subject to an external magnetic field of strength B. The interaction energy associated with a spin configuration $\mu = (\mu_0, \ldots, \mu_{N-1})$ is defined by

$$E(\mu) = -J \sum_{\substack{i,j \\ \text{neighbors}}} \mu_i \mu_j - gB \sum_i \mu_i.$$

Here each $\mu_i = \pm 1$, J is the coupling constant giving the strength of the spin-spin interactions and g is the magnetic moment of each spin. Usually, neighbors is interpreted as nearest neighbors but broader definitions are possible.

The "partition function per spin" at temperature T is defined by

$$z(J, B, T) = \Big[\sum_{\substack{\text{all} \\ \text{configurations}}} e^{-E(\mu)/kT} \Big]^{1/N}$$

for an N-site grid and k is Boltzmann's constant. Several quantities of physical interest can be expressed in terms of z. By Boltzmann's law $(e^{-E(\mu)/kT})/z^N$ is the probability of occurence of configuration μ at temperature T. The free energy per lattice site at temperature T is $-kT \log z$ and the magnetization per spin is $m = kT \frac{\partial}{\partial B} \log z$ [Tho79].

The power of the algebraic approach comes from the introduction of a matrix whose dominant eigenvalue is exactly $z_n(J, B, T)$ for a particular semi-infinite lattice with n rows. There are several matrices that can be associated with the lattice, some symmetric, others not. We use the one with the fewest nonzero entries, the duodiagonal matrix M_n of

order 2^n [Gar83]. We illustrate it for $n = 3$ and $n = 4$:

$$M_3 = \begin{bmatrix} a & & & a^{-1} & & \\ b & & & b^{-1} & & \\ & a & & & a^{-1} & \\ & b & & & b^{-1} & \\ & & b & & & b^{-1} \\ & & c & & & c^{-1} \\ & & & b & & b^{-1} \\ & & & c & & c^{-1} \end{bmatrix}$$

$$M_4 = \begin{bmatrix} a & & & & & & & a^{-1} & & & & & & & \\ b & & & & & & & b^{-1} & & & & & & & \\ & a & & & & & & & a^{-1} & & & & & & \\ & b & & & & & & & b^{-1} & & & & & & \\ & & a & & & & & & & a^{-1} & & & & & \\ & & b & & & & & & & b^{-1} & & & & & \\ & & & a & & & & & & & a^{-1} & & & & \\ & & & b & & & & & & & b^{-1} & & & & \\ & & & & b & & & & & & & b^{-1} & & & \\ & & & & c & & & & & & & c^{-1} & & & \\ & & & & & b & & & & & & & b^{-1} & & \\ & & & & & c & & & & & & & c^{-1} & & \\ & & & & & & b & & & & & & & b^{-1} & \\ & & & & & & c & & & & & & & c^{-1} & \end{bmatrix}$$

where (with appropriate normalizations)

$$a = e^{(2-B)/T}, \quad b = e^{-B/T} \text{ and } c = e^{(-2-B)/T}.$$

Since M_n acts on vectors in $\mathbf{R}^{2^n}$ by multiplication we need to index the 2^n positions in a vector and we choose a standard mechanism of using binary numbers. We give an example for $n = 5$:

$$(11010) \leftrightarrow 2^4 + 2^3 + 2^1 = 26.$$

Note that the n-bit strings here have no direct relation to the spin configurations mentioned above.

The attractive property of M_n is that it is a nonnegative irreducible matrix whose dominant eigenvalue (called the Perron root) is the wanted partition function per spin. Thus it is only necessary to approximate this eigenvalue to the desired accuracy. However the second eigenvalue and associated eigenvectors are also useful. Moreover M_n is exceedingly sparse; it has exactly 2 non-zero entries per row (and column) arranged in a regular pattern. There is only one difficulty: M_n is of order 2^n and we are interested in the case $n \to \infty$. We know of no calculations with $n \geq 20$ at present.

We note that the difficulty lies not in M_n but in the the representation of vectors in $\mathbf{R}^{2^n}$. Indeed the special structure of M_n permits evaluation of $M_n v$ for any 2^n-dimensional vector v with great efficiency. Thus M_n should be thought of, not as a matrix but as a linear operator that requires only $O(1)$ data for its definition, i.e. a constant amount of space independent of n.

Sparse vectors occur in sparse matrix work and N. Fuchs [Fuc89], when applying the Power Method to M_n, keeps only the largest 1000 entries of each vector. This device is satisfactory deep within the ferromagnetic region of the model. However after studying the Perron vector in cases near the critical temperature we found that it contained almost no small entries.

As a substitute for sparsity we propose to limit the number of distinct values that can occur among a vector's components. In technical terms we select a finite family of *indicial* subspaces $\{\mathcal{C}_i\}$, each of which is spanned by an orthogonal basis of *indicial* vectors $\{x_1, \ldots, x_m\}$ such that the nonzero entries of each x_i are ones, and the positions of the nonzero entries of x_i and x_j, $i \neq j$, are disjoint. We then approximate the top two column eigenvectors of M_n from a member of $\{\mathcal{C}_i\}$. The top two row eigenvectors are approximated using a dual family $\{\mathcal{R}_i\}$.

We indicate briefly how the two families of indicial subspaces can be used to obtain a *minimal representation* for the top two eigenvectors of M_n [PH91].

Step 1. Select $\mathcal{C}_i$ and $\mathcal{R}_i$ from the two families. Also represent, in compact form, the orthogonal projection P of the transfer matrix M_n onto the subspace $\mathcal{C}_i$. In addition represent the projection Q of the adjoint matrix M_n^* onto the subspace $\mathcal{R}_i$.

Step 2. Compute the two largest eigenvalues and the associated row and column eigenvec-

tors of P and Q. These are, in a sense, the best approximations from the given pair of indicial subspaces $\mathcal{C}_i$ and $\mathcal{R}_i$. However they may not be good enough.

Step 3. Evaluate residual norms, condition numbers and associated error bounds and estimates. If the estimates are satisfactory then compute the required properties of the model and stop. Otherwise return to Step 1 with the next member of each family.

We now discuss our choice of indicial subspaces for approximating the column eigenvectors of M_n. In particular, we describe how we decide which entries of the eigenvector should be forced to have the same value.

Consider the expression for the energy associated with a particular state $\mu = (\mu_1, \ldots, \mu_n)$, $\mu_j = \pm 1$, in a 1D Ising model with only n sites:

$$E(\mu) = -(J \sum_{i=1}^{n-1} \mu_i \mu_{i+1} + gB \sum_{i=1}^{n} \mu_i).$$

Observe that in the first sum, -1 occurs t times if there are t transitions (adjacent changes of sign) in the configuration μ. Thus

$$\sum_{i=1}^{n-1} \mu_i \mu_{i+1} = n - 1 - 2t.$$

Similarly

$$\sum_{i=1}^{n} \mu_i = k - (n - k) = 2k - n$$

if there are exactly k $+1$'s in μ. Thus two states μ and $\bar{\mu}$ contribute equally to the associated partition function if they have the same number of $+1$'s and the same number of transitions.

The idea of using k and t can be applied to the 2D model. However, the situation is more complicated here and we do not know how to justify the special role of k and t. Nevertheless, numerical evidence does indicate the utility of k and t.

Table 1.1 shows the dominant (Perron) column eigenvector for M_5 with parameter settings $B = 0.0001$ and $T = 2.2$, which is within 4% of the critical temperature T_c. The eigenvector has been normalized to have largest entry 1, and the entries of the table have been sorted in decreasing value of the components of the eigenvector. The first column of the table shows the index of a position in the eigenvector, written as a 5-bit binary number (and with its decimal equivalent in parenthesis), and the second and third columns give the value of k and t for that index. The last column gives the value of that component of the eigenvector. We shall write the indices as binary numbers in the following discussion.

	position	k	t	value
	11111 (31)	5	0	1.0000000
	00000 (0)	0	0	0.9967231
	10111 (23)	4	2	0.5597178
	01000 (8)	1	2	0.5583141
	11011 (27)	4	2	0.5487801
	00100 (4)	1	2	0.5473442
	11101 (29)	4	2	0.5352361
	00010 (2)	1	2	0.5337697
‡	11110 (30)	4	1	0.5059892
†	00001 (1)	1	1	0.5045102
	10011 (19)	3	2	0.4027520
	01100 (12)	2	2	0.4022891
	11001 (25)	3	2	0.3743792
	00110 (6)	2	2	0.3738325
	01110 (14)	3	2	0.3522495
	10001 (17)	2	2	0.3521065
	10101 (21)	3	4	0.3420300
	01010 (10)	2	4	0.3415416
	11100 (28)	3	1	0.3286180
	00011 (3)	2	1	0.3279917
‡	01111 (15)	4	1	0.3214520
†	10000 (16)	1	1	0.3209276
	10110 (22)	3	3	0.3048252
	11010 (26)	3	3	0.3044408
	01001 (9)	2	3	0.3042764
	00101 (5)	2	3	0.3038702
	11000 (24)	2	1	0.2798594
	00111 (7)	3	1	0.2797993
	10010 (18)	2	3	0.2598551
	01101 (13)	3	3	0.2598535
	10100 (20)	2	3	0.2473428
	01011 (11)	3	3	0.2473127

Table 1.1: Perron eigenvector for M_5 with $B = 0.0001$, $T = 2.2$

We see from the table that although the eigenvector is not sparse, those positions with the same values of k and t have component values that are quite close. For example, the positions with 4 ones and 2 bit transitions are 10111, 11011 and 11101, and their component values are 0.5597178, 0.5487801 and 0.5352361 respectively.

A careful look at the table, however, reveals an anomaly. The positions 00001 and 10000 both have a single one and a single bit transition, but their values are very different: 0.5045102 and 0.3209276 respectively (see the items marked †). The same problem occurs with positions 11110 and 01111 (items marked ‡). This anomaly occurs more frequently for higher n's, and shows that using k and t as the sole criteria for forcing equality in eigenvector components is inadequate.

Observe, however, that for each anomalous pair, the two positions have different trailing bit. This suggests using the trailing bit as a third criterion. More generally, we can use the last l bits of each index.

With each value of l, we can define an indicial subspace $\mathcal{C}_l \subseteq \mathbf{R}^{2^n}$ for which $x \in \mathcal{C}_l$ has the same value in entries i and j if the binary representations of i and j have the same number of 1s, the same number of bit transitions, and the same last l bits. We obtain a dual subspace $\mathcal{R}_l$ for approximating the row eigenvectors of M_n by using the first l bits of an index as the third criterion.

We note that there is a tradeoff present in choosing approximating subspaces. By forcing equality, we reduce the dimension of the subspaces that we work in, but at the same time, we sacrifice the accuracy of our results. A discussion of the approximating properties of our indicial subspaces is found in [PH91]. We briefly state some results from there.

For the case $n \leq 15$, we were able to compare our approximations with the exact results. In our first implementation, we obtained approximations that were accurate to 7 decimal places for $n = 14$, using a subspace of dimension only 896 as compared to $2^{14} = 16384$. We also ran the code for $n > 20$ (for which no exact results are available), and our error estimates showed that the subspaces delivered reasonable approximations. For example, for $n = 30$, the approximations were estimated to be good to at least 4 decimal places using a subspace of dimension as small as 5632 (note that $2^{30} \approx 10^9$).

We now give an overview of the thesis.

Chapter 2 formalizes the idea of indicial subspaces and analyzes the structural properties of the projections of M_n onto such subspaces. In Section 2.1, we define the building blocks of indicial subspaces, and in Section 2.2, we show how approximations can

be derived from these subspaces. We then study the action of M_n on our indicial subspaces in Section 2.3, and this enables us to analyze the structure of the projections of M_n in Sections 2.4 and 2.5. We shall show that in general, the projections of M_n are also *sparse* with either 2 or 4 nonzeros per column. Finally, in Sections 2.6 and 2.7, we introduce a more general class of indicial subspaces, and show that the ones we have used are the best in the class.

Chapter 3 is concerned with the combinatorics of indicial subspaces. We begin by analyzing a restricted class of indicial subspaces in Section 3.1, where we will determine the dimension of those subspaces and the maximum number of components that are forced to be equal. We then extend the results to arbitrary indicial subspaces in Sections 3.2 and 3.3. The key result in that chapter is that our indicial subspaces have dimension $O(n^2 2^{l-1})$.

Appendix A considers how we can extend the results of Chapter 3 to the more general class of indicial subspaces introduced in Section 2.6.

1.2 Basic Notation and Terminology

We will follow Householder's conventions: upper case Roman letters for matrices, lower case letters for column vectors, and lower case Greek letters for scalars. However, the letters i, j, k, l, m, n and t will be reserved for integers. All matrices and vectors will be real. The transpose of A will be denoted by A^*, and the inner product of vectors x and y by $\langle x, y \rangle = x^* y$. We will exclusively use the Euclidean norm for vectors: $\|x\| = \sqrt{x^* x}$.

As the theory behind our indicial subspaces is intimately connected with the binary representations of numbers, we will index the rows and columns of a matrix, and the elements of a vector, starting from 0, unless otherwise specified. Thus for $A \in \mathbf{R}^{l \times m}$ and $x \in \mathbf{R}^m$, $(A)_{i,j}$ denotes the entry in row i and column j of A, $0 \le i \le l-1$, $0 \le j \le m-1$, and $x(i)$ denotes the i^{th} element of x, $0 \le i \le m-1$.

The $l \times m$ zero and identity matrices will be written as $O_{l \times m}$ and $I_{l \times m}$ respectively; the $2^n \times 2^n$ identity matrix will be written as I_n. For $Q \in \mathbf{R}^{l \times m}$, we let span$(Q)$ denote the subspace of $\mathbf{R}^l$ spanned by the m columns of Q. Similarly, if $\mathcal{S}$ is a set of vectors in $\mathbf{R}^l$, the subspace spanned by these vectors will be denoted by span$(\mathcal{S})$.

The symbol := will denote a definition, and the symbol $\square$ will mark the end of a proof.

By a (binary) string ω, we shall mean a finite sequence of 0s and 1s. The empty

string is denoted by ε. We write $\{0,1\}^*$ for the set of all strings (including ε), and $\{0,1\}^n$ for the set of n-bit strings, $n \geq 1$. The length of a string ω is denoted by $|\omega|$, the concatenation of two strings ω_1 and ω_2 by $\omega_1 \circ \omega_2$, and the reversal of a string ω (i.e. ω written backwards) by ω^R.

$$\text{eg.} \quad \{0,1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\},$$
$$|001101| = 6, \quad 010 \circ 110 = 010110, \quad 001101^R = 101100.$$

We also define $|\varepsilon| := 0$, $\varepsilon^r := \varepsilon$, and $\varepsilon \circ \omega = \omega \circ \varepsilon := \omega$ for any string ω.

For a nonempty string ω, we denote its i^{th} bit from the left by $w(i)$, $i = 1, 2, \ldots, |\omega|$. Thus $\omega = \omega(1) \circ \omega(2) \circ \cdots \circ \omega(|\omega|)$, and $\omega^R = \omega(|\omega|) \circ \omega(|\omega| - 1) \circ \cdots \circ \omega(1)$. For given l, $1 \leq l \leq |\omega|$, the l-bit prefix of ω is the substring $\omega(1) \circ \omega(2) \circ \cdots \circ \omega(l)$, and the l-bit suffix of ω is the substring $\omega(|\omega| - l + 1) \circ \omega(|\omega| - l + 2) \circ \cdots \circ \omega(|\omega|)$. The empty string ε will be considered to be the 0-bit prefix and the 0-bit suffix of any string ω. We shall also refer to $\omega(1)$, $\omega(1) \circ \omega(2)$ and $\omega(|\omega|)$ as the leading bit, leading bit pair and trailing bit respectively of a string ω with $|\omega| \geq 2$.

There is a natural correspondence between binary strings and the nonnegative integers $\mathbf{N}$ arising from the concept of the binary representation of numbers. We formalize this by defining two functions:

$$v : \{0,1\}^* \to \mathbf{N} \text{ mapping } \omega \in \{0,1\}^* \text{ to the integer value it represents } (v(\varepsilon) := 0),$$

and for $n \geq 1$,

$$\sigma_n : \{0, 1, \ldots, 2^n - 1\} \to \{0,1\}^n \text{ mapping } i \in \mathbf{N} \text{ to its } n\text{-bit binary representation.}$$

We note that there is no uniqueness in these maps: two different strings may have the same value under v, eg. $v(011) = v(11) = 3$, and a nonnegative integer is mapped to different strings under different σ_n's, eg. $\sigma_2(3) = 11$, $\sigma_3(3) = 011$. This, however, should cause no confusion. We can extend v to sets of strings: $v(\mathbf{E}) = \{v(\omega) : \omega \in \mathbf{E}\}$, $\mathbf{E} \subseteq \{0,1\}^n, n \geq 1$.

Two other properties of binary strings that are of interest to us are their 1-bit counts and bit transition counts.

Definition 1.1 *Let ω be a nonempty string. We define $\kappa(\omega)$ to be the number of 1s appearing in ω, and $\tau(\omega)$ to be the number of bit transitions in ω (i.e. 0 to 1 or 1 to 0). We also define $\kappa(\varepsilon) := 0$ and $\tau(\varepsilon) := 0$.*

eg. $\kappa(000000) = 0, \quad \kappa(111111) = 6, \quad \kappa(101101) = 4,$

$\tau(000000) = \tau(111111) = 0, \quad \tau(001111) = 1, \quad \tau(101101) = 4, \quad \tau(010101) = 5.$

We note that for $\omega \in \{0,1\}^n$, we have $0 \leq \kappa(\omega) \leq n$ and $0 \leq \tau(\omega) \leq n-1$.

It should be emphasized that the functions κ and τ are defined for binary strings, and not for the binary representation of numbers. The earlier remarks on the non-uniqueness of binary representations apply here. In particular, the bit transition count associated with a number depends on the choice of the binary representation. Thus, $\tau(\sigma_2(3)) = \tau(11) = 0$ but $\tau(\sigma_3(3)) = \tau(011) = 1$. This issue should be kept in mind in any implementation of indicial subspaces.

Chapter 2

Projections of Transfer Matrices onto Indicial Subspaces

2.1 Indicial sets, vectors and bases

We begin by defining the building blocks of our indicial subspaces. Each such subspace is obtained by forcing two vector components to have the same value if the binary representation of their indices have the same number of 1's, the same number of bit transitions and the same l-bit suffixes, where l is a fixed nonnegative integer. By grouping the indices of equal-valued components together, we obtain a partition of the collection of indices, and an associated basis for the subspace.

We first illustrate the ideas with a simple example where no suffixes are involved. The space we shall work in is $\mathbf{R}^8$ and we shall regard indices as 3-bit binary strings. Consider the subspace $\mathcal{C}$ of $\mathbf{R}^8$ obtained by forcing two components to have the same value if their indices have the same 1-bit count and the same bit transition count. It is easily verified that among the eight 3-bit strings $000, \ldots, 111$, there are only two pairs of strings, namely $\{001, 100\}$ and $\{011, 110\}$, which satisfy the above criteria. By grouping the indices of equal-valued components together, we have the following partition of $\{000, \ldots, 111\}$:

$$\{\{000\}, \{001, 100\}, \{010\}, \{011, 110\}, \{101\}, \{111\}\}. \tag{2.1}$$

We call each member of the partition an *indicial set*. To each indicial set $\mathbf{I}$, we can associate an *indicial vector* x, which has ones in positions whose indices are in $\mathbf{I}$, and zeros elsewhere.

For the partition (2.1), we have the following indicial vectors:

$$x_1 = (1\,0\,0\,0\,0\,0\,0\,0)^*,\ x_2 = (0\,1\,0\,0\,1\,0\,0\,0)^*,\ x_3 = (0\,0\,1\,0\,0\,0\,0\,0)^*,$$
$$x_4 = (0\,0\,0\,1\,0\,0\,1\,0)^*,\ x_5 = (0\,0\,0\,0\,0\,1\,0\,0)^*,\ x_6 = (0\,0\,0\,0\,0\,0\,0\,1)^*\}.$$

A moment's thought will reveal that $\{x_1, \ldots, x_6\}$ is a *basis* for the subspace C.

Formally, we define

Definition 2.1 *Let $n \geq 1$, $0 \leq k \leq n$, $0 \leq t \leq n-1$, and $\omega \in \{0,1\}^*$ with $|\omega| \leq n$. Define*

$$\mathbf{I}^n_{\omega,k,t} := \{\mu \in \{0,1\}^n : \kappa(\mu) = k,\ \tau(\mu) = t,\ \textit{and } \omega \textit{ is the } |\omega|\textit{-bit suffix of } \mu\}.$$

$\mathbf{I}^n_{\omega,k,t}$ *is called a* suffix-based indicial set. *For a given $\omega \in \{0,1\}^*$ with $|\omega| \leq n$, we call a pair k, t* admissible *if $\mathbf{I}^n_{\omega,k,t} \neq \emptyset$.*

$$\text{eg.}\quad \mathbf{I}^4_{\epsilon,0,0} = \{0000\},\quad \mathbf{I}^4_{1,3,2} = \{1011, 1101\},\quad \mathbf{I}^4_{01,2,2} = \{1001\}.$$

We leave it as an exercise for the reader to verify that $\mathbf{I}^4_{1,3,3} = \emptyset$.

Definition 2.2 *Suppose $\mathbf{E} \subseteq \{0,1\}^n$, $n \geq 1$. Define the vector $x_{\mathbf{E}} \in \mathbf{R}^{2^n}$ by:*

$$x_{\mathbf{E}}(i) := \begin{cases} 1 & \textit{if } \sigma_n(i) \in \mathbf{E} \\ 0 & \textit{if } \sigma_n(i) \notin \mathbf{E} \end{cases} \qquad 0 \leq i \leq 2^n - 1.$$

$x_{\mathbf{E}}$ can be regarded as the tabulation of the characteristic function $\chi_{\mathbf{E}}$ of $\mathbf{E}$. If $\mathbf{E}$ is a suffix-based indicial set, i.e. $\mathbf{E} = \mathbf{I}^n_{\omega,k,t}$ for some ω, k and t, we call $x_{\mathbf{E}}$ a suffix-based indicial vector *and we also write it as $x^n_{\omega,k,t}$. Note that $x_\emptyset = 0$, and that $\|x_{\mathbf{E}}\|^2 = |\mathbf{E}|$.*

Definition 2.3 *Let $n \geq 1$, $0 \leq l \leq n$. Define*

$$\mathcal{S}_{n,l} := \{x^n_{\omega,k,t} : |\omega| = l,\ k,t \textit{ admissible}\}.$$

We call $\mathcal{S}_{n,l}$ an indicial basis *and* span*$(\mathcal{S}_{n,l})$ an* indicial subspace.

We rework the illustrative example using our new terminology:

$$\text{eg.}\quad \mathbf{I}^3_{\epsilon,0,0} = \{000\},\ \mathbf{I}^3_{\epsilon,1,1} = \{001, 100\},\ \mathbf{I}^3_{\epsilon,1,2} = \{010\},$$
$$\mathbf{I}^3_{\epsilon,2,1} = \{011, 110\},\ \mathbf{I}^3_{\epsilon,2,2} = \{101\},\ \mathbf{I}^3_{\epsilon,3,0} = \{111\},$$
$$\mathcal{S}_{3,0} = \{(1\,0\,0\,0\,0\,0\,0\,0)^*, (0\,1\,0\,0\,1\,0\,0\,0)^*, (0\,0\,1\,0\,0\,0\,0\,0)^*,$$
$$(0\,0\,0\,1\,0\,0\,1\,0)^*, (0\,0\,0\,0\,0\,1\,0\,0)^*, (0\,0\,0\,0\,0\,0\,0\,1)^*\}.$$

Central to our analysis of the action of the transfer matrix on indicial bases (see Section 2.3) are the following two types of operators on sets of binary strings. The first type will enable us to relate the image of an indicial vector under the transfer matrix to another indicial vector; the second type plays a role in the decoupling of the action of the transfer matrix. We urge the reader to read with care the definitions of 2ω and $2\omega + 1$ below.

Definition 2.4 *For a nonempty string ω, the strings 2ω and $2\omega + 1$ are defined by:*

$$\begin{aligned} 2\omega &:= \omega(2) \circ \omega(3) \circ \cdots \circ \omega(|\omega|) \circ 0 \\ \textit{and} \qquad 2\omega + 1 &:= \omega(2) \circ \omega(3) \circ \cdots \circ \omega(|\omega|) \circ 1. \end{aligned}$$

It is easily verified that $v(2\omega) = 2v(\omega) \bmod 2^{|\omega|}$ and $v(2\omega + 1) = (2v(\omega) + 1) \bmod 2^{|\omega|}$. We extend the definition to sets of strings: for $\mathbf{E} \subseteq \{0,1\}^n$, $n \geq 1$,

$$2\mathbf{E} := \{2\omega : \omega \in \mathbf{E}\} \quad \textit{and} \quad 2\mathbf{E} + 1 := \{2\omega + 1 : \omega \in \mathbf{E}\}.$$

The reader familiar with binary arithmetic will recall that multiplying a number ω by 2 corresponds to shifting in a 0 from the right, and that multiplying ω by 2 and then adding 1 corresponds to shifting in a 1. The strings 2ω and $2\omega + 1$ are the results we would obtain when we perform the operations in a computer with $|\omega|$-bit words.

Definition 2.5 *Let $\mathbf{E} \subseteq \{0,1\}^n$, $n \geq 2$. We define*

$$\begin{aligned} \mathbf{E}^0 &:= \{\omega \in \mathbf{E} : \omega(2) = 0\} \\ \textit{and} \qquad \mathbf{E}^1 &:= \{\omega \in \mathbf{E} : \omega(2) = 1\}, \end{aligned}$$

i.e. $\mathbf{E}^0$ and $\mathbf{E}^1$ are subsets of strings in $\mathbf{E}$ having 2^{nd} leading bit 0 and 1 respectively. It follows from the definition that $\mathbf{E}$ is the disjoint union of $\mathbf{E}^0$ and $\mathbf{E}^1$. If $\mathbf{E} = \mathbf{I}^n_{\omega,k,t}$, we also write $\mathbf{E}^0 = \mathbf{I}^{n,0}_{\omega,k,t}$ and $\mathbf{E}^1 = \mathbf{I}^{n,1}_{\omega,k,t}$.

eg. $\mathbf{E} = \{0011, 0100, 0101, 1000\}$, $\mathbf{E}^0 = \{0011, 1000\}$, $\mathbf{E}^1 = \{0100, 0101\}$.
$\mathbf{E} = \{0010, 0011\}$, $\mathbf{E}^0 = \mathbf{E}$, $\mathbf{E}^1 = \emptyset$.

$\mathbf{E} = \mathbf{I}^7_{1,3,3} = \{0001011, 0001101, 0010011, 0011001, 0100011, 0110001\}$,
$\mathbf{E}^0 = \{0001011, 0001101, 0010011, 0011001\}$, $\mathbf{E}^1 = \{0100011, 0110001\}$,

$$2\mathbf{E}^0 = \{0010110, 0011010, 0100110, 0110010\} = \mathbf{I}^7_{10,3,4},$$
$$2\mathbf{E}^0 + 1 = \{0010111, 0011011, 0100111, 0110011\} = \mathbf{I}^7_{11,4,3},$$
$$2\mathbf{E}^1 = \{1000110, 1100010\} = \mathbf{I}^7_{10,3,3},$$
$$2\mathbf{E}^1 + 1 = \{1000111, 1100011\} = \mathbf{I}^7_{11,4,2}.$$

As the last example indicates, $2\mathbf{E}^0$, $2\mathbf{E}^0 + 1$, $2\mathbf{E}^1$ and $2\mathbf{E}^1 + 1$ are pairwise disjoint and are themselves suffix-based indicial sets, and $|2\mathbf{E}^0| = |2\mathbf{E}^0 + 1| = |\mathbf{E}^0|$ and $|2\mathbf{E}^1| = |2\mathbf{E}^1 + 1| = |\mathbf{E}^1|$. This is true in general (see Proposition 2.1.6 and Theorems 2.1.7 and 2.1.8 below).

In discussions where the value of n is assumed fixed, we will omit it in writing indicial objects. Thus, we write $\mathbf{I}_{\omega,k,t}$, $x_{\omega,k,t}$, $\mathbf{I}^0_{\omega,k,t}$ and $\mathbf{I}^1_{\omega,k,t}$ instead of $\mathbf{I}^n_{\omega,k,t}$, $x^n_{\omega,k,t}$, $\mathbf{I}^{n,0}_{\omega,k,t}$ and $\mathbf{I}^{n,1}_{\omega,k,t}$ respectively.

In an analogous fashion, we can define prefix-based indicial sets $\mathbf{J}^n_{\omega,k,t}$, vectors $y^n_{\omega,k,t}$ and bases $\mathcal{T}_{n,l}$. It turns out, however, that prefix-based indicial objects can be derived from corresponding suffix-based ones. This will be explored in Section 2.4.

We note here for future analyses some crucial properties of suffix-based indicial sets, vectors and bases. We urge the reader to go through them carefully, with the exception of the proof of Theorem 2.1.8, where parts (b), (c) and (d) may be skipped.

Fundamental Properties

Proposition 2.1.1 *For fixed n and $|\omega|$, the nonempty indicial sets $\mathbf{I}^n_{\omega,k,t}$ are disjoint. Thus for $0 \le l \le n$, $\mathcal{S}_{n,l}$ is an orthogonal basis (i.e. for $x, y \in \mathcal{S}_{n,l}$, $x \ne y \Rightarrow x^*y = 0$) and so is linearly independent.*

Proposition 2.1.2 *For fixed n and $|\omega|$, the collection of nonempty indicial sets $\mathbf{I}^n_{\omega,k,t}$ is a partition of $\{0,1\}^n$. Thus for each $0 \le i \le 2^n - 1$, there is a unique $x \in \mathcal{S}_{n,l}$ with $x(i) = 1$.*

Proposition 2.1.3 *The trailing bit and the parity of the transition count of a nonempty string μ determines its leading bit.*

Proof. An even number of transitions (viewing from the right end of μ to its left end) restores its trailing bit whereas an odd number of transitions reverses its trailing bit. □

Proposition 2.1.4 *The strings in each indicial set $\mathbf{I}^n_{\omega,k,t}$, $n \ge 2$, $\omega \ne \varepsilon$, all have the same leading bit since:*

(a) the trailing bit of ω determines the trailing bit of each $\mu \in \mathbf{I}^n_{\omega,k,t}$,

(b) by Proposition 2.1.3, if t is even, the leading bit of each $\mu \in \mathbf{I}^n_{\omega,k,t}$ must be the same as its trailing bit; if t is odd, the leading bit must be different.

Proposition 2.1.5 *The strings in each $\mathbf{I}^{n,0}_{\omega,k,t}$, $n \geq 3$, $\omega \neq \varepsilon$, all have the same leading bit pair and the same trailing bit since Proposition 2.1.4 determines the leading and trailing bit, and the 2^{nd} leading bit is 0 by definition. Similarly, the strings in each $\mathbf{I}^{n,1}_{\omega,k,t}$, $n \geq 3$, $\omega \neq \varepsilon$, all have the same leading bit pair and the same trailing bit.*

Proposition 2.1.6 *Let $\mathbf{E} \subseteq \{0,1\}^n$, $n \geq 2$. The sets $2\mathbf{E}^0$, $2\mathbf{E}^0 + 1$, $2\mathbf{E}^1$ and $2\mathbf{E}^1 + 1$ are pairwise disjoint since by definition:*

(a) strings in $2\mathbf{E}^0$ have leading bit 0 and trailing bit 0

(b) strings in $2\mathbf{E}^0 + 1$ have leading bit 0 and trailing bit 1

(c) strings in $2\mathbf{E}^1$ have leading bit 1 and trailing bit 0

(d) strings in $2\mathbf{E}^1 + 1$ have leading bit 1 and trailing bit 1

Theorem 2.1.7 *Let $\mathbf{E} = \mathbf{I}^n_{\omega,k,t}$, $n \geq 2$, $\omega \neq \varepsilon$. Then $|2\mathbf{E}^0| = |2\mathbf{E}^0 + 1| = |\mathbf{E}^0|$ and $|2\mathbf{E}^1| = |2\mathbf{E}^1 + 1| = |\mathbf{E}^1|$.*

Proof. Let $\omega_1, \omega_2 \in \mathbf{E}^0$ with $2\omega_1 = 2\omega_2$. Then

$$\omega_1(2) \circ \omega_1(3) \circ \cdots \circ \omega_1(n) \circ 0 = \omega_2(2) \circ \omega_2(3) \circ \cdots \circ \omega_2(n) \circ 0$$

and so

$$\omega_1 = \omega_1(1) \circ \omega_1(2) \circ \cdots \circ \omega_1(n) = \omega_2(1) \circ \omega_2(2) \circ \cdots \circ \omega_2(n) = \omega_2$$

since $\omega_1(1) = \omega_2(1)$ by Proposition 2.1.4 (note that $\omega_1, \omega_2 \in \mathbf{E}$). Therefore, for $\omega_1, \omega_2 \in \mathbf{E}^0$, $\omega_1 \neq \omega_2 \Rightarrow 2\omega_1 \neq 2\omega_2$, and we have a one-to-one correspondence between $\mathbf{E}^0$ and $2\mathbf{E}^0$. So $|2\mathbf{E}^0| = |\mathbf{E}^0|$. Similarly, we have $|2\mathbf{E}^0 + 1| = |\mathbf{E}^0|$ and $|2\mathbf{E}^1| = |2\mathbf{E}^1 + 1| = |\mathbf{E}^1|$. □

Theorem 2.1.8 *Let $\mathbf{E} = \mathbf{I}^n_{\omega,k,t}$, $n \geq 3$, $0 < |\omega| < n$. Then $2\mathbf{E}^0$, $2\mathbf{E}^0 + 1$, $2\mathbf{E}^1$ and $2\mathbf{E}^1 + 1$ are themselves suffix-based indicial sets.*

Proof. There are four cases to consider, depending on the trailing bit of ω and the parity of t. We will prove the result for the first case; the proofs for the remaining three cases are similar.

a) trailing bit of ω is 0 and t is even:

We claim that $2\mathbf{E}^0 = \mathbf{I}^n_{\omega\circ 0,k,t}$. Suppose $\mu \in \mathbf{E}^0 \subseteq \mathbf{E}$. Then $\mu(2) = 0$, $\mu(n) = 0$, and by Proposition 2.1.4 applied to $\mathbf{E}$, $\mu(1) = 0$. It is clear that μ and 2μ have the same 1-bit count and the same transition count, and that $\omega \circ 0$ is the $(|\omega| + 1)$-bit suffix of 2μ. So $2\mu \in \mathbf{I}^n_{\omega\circ 0,k,t}$, and $2\mathbf{E}^0 \subseteq \mathbf{I}^n_{\omega\circ 0,k,t}$.

Conversely, let $\mu' \in \mathbf{I}^n_{\omega\circ 0,k,t}$. Then by definition, $\mu'(n) = 0$ and $\mu'(n-1) = \omega(|\omega|) = 0$. By Proposition 2.1.4 applied to $\mathbf{I}^n_{\omega\circ 0,k,t}$, $\mu'(1) = 0$. Thus $\mu' = 0\circ\mu'(2)\circ\cdots\circ\mu'(n-2)\circ 0\circ 0$. If we let $\mu = 0\circ 0\circ\mu'(2)\circ\cdots\circ\mu'(n-2)\circ 0$, we see that $\mu' = 2\mu$. It is clear that μ and μ' have the same 1-bit count and the same transition count. So $\mu \in \mathbf{I}^n_{\omega,k,t} = \mathbf{E}^0$, and $\mathbf{I}^n_{\omega\circ 0,k,t} \subseteq 2\mathbf{E}^0$. Therefore, we have $2\mathbf{E}^0 = \mathbf{I}^n_{\omega\circ 0,k,t}$. We can show in a similar manner that:

$$2\mathbf{E}^0 + 1 = \mathbf{I}^n_{\omega\circ 1,k+1,t+1},\ 2\mathbf{E}^1 = \mathbf{I}^n_{\omega\circ 0,k,t-1},\ 2\mathbf{E}^1 + 1 = \mathbf{I}^n_{\omega\circ 1,k+1,t}.$$

b) trailing bit of ω is 0 and t is odd:

$$\begin{aligned} 2\mathbf{E}^0 &= \mathbf{I}^n_{\omega\circ 0,k-1,t-1}, & 2\mathbf{E}^0 + 1 &= \mathbf{I}^n_{\omega\circ 1,k,t}, \\ 2\mathbf{E}^1 &= \mathbf{I}^n_{\omega\circ 0,k-1,t}, & 2\mathbf{E}^1 + 1 &= \mathbf{I}^n_{\omega\circ 1,k,t+1}. \end{aligned}$$

c) trailing bit of ω is 1 and t is even:

$$\begin{aligned} 2\mathbf{E}^0 &= \mathbf{I}^n_{\omega\circ 0,k-1,t}, & 2\mathbf{E}^0 + 1 &= \mathbf{I}^n_{\omega\circ 1,k,t-1}, \\ 2\mathbf{E}^1 &= \mathbf{I}^n_{\omega\circ 0,k-1,t+1}, & 2\mathbf{E}^1 + 1 &= \mathbf{I}^n_{\omega\circ 1,k,t}. \end{aligned}$$

d) trailing bit of ω is 1 and t is odd:

$$\begin{aligned} 2\mathbf{E}^0 &= \mathbf{I}^n_{\omega\circ 0,k,t+1}, & 2\mathbf{E}^0 + 1 &= \mathbf{I}^n_{\omega\circ 1,k+1,t}, \\ 2\mathbf{E}^1 &= \mathbf{I}^n_{\omega\circ 0,k,t}, & 2\mathbf{E}^1 + 1 &= \mathbf{I}^n_{\omega\circ 1,k+1,t-1}. \end{aligned}$$ □

2.2 Subspace Approximations

The orthogonal basis $\mathcal{S}_{n,t}$ was defined in the previous section. There is a unique orthogonal projection of M_n onto $\mathrm{span}(\mathcal{S}_{n,t})$ and our method takes the two largest eigenvalues of this projection as approximations to those of M_n.

Here are the details.

Let $X \in \mathbf{R}^{2^n \times |\mathcal{S}_{n,l}|}$ be a matrix whose columns are the vectors in $\mathcal{S}_{n,l}$. Let $X^*X = D_X$, a positive definite diagonal matrix (with integer entries). Let $\tilde{X} = XD_X^{-1/2}$. The projector on $\mathcal{S}_{n,l}$ is $\tilde{X}\tilde{X}^*$, and the projection of M_n is $\tilde{X}\tilde{X}^*M_n\tilde{X}\tilde{X}^*$, and its representation in the basis given by $\tilde{X}$ is

$$\tilde{P}^C_{n,l} = \tilde{X}^*M_n\tilde{X} = D_X^{-1/2}X^*M_nXD_X^{-1/2}.$$

Observe that $\tilde{P}^C_{n,l}$ is diagonally similar to

$$P^C_{n,l} = D_X^{-1}X^*M_nX = D_X^{-1/2}\tilde{P}^C_{n,l}D_X^{1/2}.$$

It is slightly more convenient to work with $P^C_{n,l}$ than with $\tilde{P}^C_{n,l}$.

In order to obtain good error estimates we approximate M_n^* as well but for reasons discussed in Section 2.7 we project it onto the subspace $\mathcal{T}_{n,l}$ dual to $\mathcal{S}_{n,l}$. If Y is a matrix whose columns are the vectors in $\mathcal{T}_{n,l}$ we compute the representation of the orthogonal projection of M_n^* as

$$P^R_{n,l} = D_Y^{-1}Y^*M_n^*Y.$$

Let π_1 and π_2 be the largest two eigenvalues of $P^C_{n,l}$. In the absence of two such positive eigenvalues we abandon the basis $\mathcal{S}_{n,l}$ immediately and increase l by 1. Thus we compute (π_i, g_i, h_i^*), $i = 1, 2$,

$$P^C_{n,l}g_1 = g_1\pi_1, \quad h_1^*P^C_{n,l} = \pi_1h_1^*, \quad P^C_{n,l}g_2 = g_2\pi_2, \quad h_2^*P^C_{n,l} = \pi_2h_2^*, \quad 0 < \pi_2 < \pi_1.$$

Approximate eigenelements for M_n are defined as

$$(\pi_i, Xg_i, h_i^*D_X^{-1}X^*), \quad i = 1, 2,$$

although we may not wish to form these eigenvectors until we are confident that they are satisfactory. We define similar approximations for M_n^* using the basis $\mathcal{T}_{n,l}$.

2.3 Action of duodiagonal matrices on indicial bases

Our primary goal is to analyze the structure of the column projection matrix $P^C_{n,l}$ and of the row projection matrix $P^R_{n,l}$. This requires us to understand the action of the

transfer matrix M_n on basis vectors x in $\mathcal{S}_{n,l}$ for $l \geq 1$. In this section, we shall see how to decouple the action of M_n, and thus express $M_n x$ as a linear combination of indicial vectors. Section 2.4 then analyzes the structure of $P^C_{n,l}$ and $P^R_{n,l}$ for $l \geq 1$. The degenerate case $l = 0$ will be discussed in Section 2.5.

Let n be a fixed integer ≥ 3, and l be a fixed integer ≥ 1. Recall that $P^C_{n,l} = D_X^{-1} X^* M_n X$ where the columns of X are vectors in $\mathcal{S}_{n,l}$, and $D_X = X^* X$. To elucidate the action of M_n on X, we introduce a general class of duodiagonal matrices U_n, of which M_n is a special case. We first illustrate it for $n = 4$:

$$U_4 := \begin{bmatrix}
u_0^0 & & & & & & & & u_2^0 & & & & & & & \\
u_0^1 & & & & & & & & u_2^1 & & & & & & & \\
 & u_0^2 & & & & & & & & u_2^2 & & & & & & \\
 & u_0^3 & & & & & & & & u_2^3 & & & & & & \\
 & & u_0^0 & & & & & & & & u_2^0 & & & & & \\
 & & u_0^1 & & & & & & & & u_2^1 & & & & & \\
 & & & u_0^2 & & & & & & & & u_2^2 & & & & \\
 & & & u_0^3 & & & & & & & & u_2^3 & & & & \\
 & & & & u_1^0 & & & & & & & & u_3^0 & & & \\
 & & & & u_1^1 & & & & & & & & u_3^1 & & & \\
 & & & & & u_1^2 & & & & & & & & u_3^2 & & \\
 & & & & & u_1^3 & & & & & & & & u_3^3 & & \\
 & & & & & & u_1^0 & & & & & & & & u_3^0 & \\
 & & & & & & u_1^1 & & & & & & & & u_3^1 & \\
 & & & & & & & u_1^2 & & & & & & & & u_3^2 \\
 & & & & & & & u_1^3 & & & & & & & & u_3^3
\end{bmatrix}.$$

In general, we consider the $2^n \times 2^n$ duodiagonal matrix:

$$U_n := \begin{bmatrix} U_n^{(0)} & O_{2^{n-1} \times 2^{n-2}} & U_n^{(2)} & O_{2^{n-1} \times 2^{n-2}} \\ O_{2^{n-1} \times 2^{n-2}} & U_n^{(1)} & O_{2^{n-1} \times 2^{n-2}} & U_n^{(3)} \end{bmatrix}$$

where

$$U_n^{(0)} = \begin{bmatrix} U^{(0)} & & \bigcirc \\ & U^{(0)} & \\ & & \ddots \\ \bigcirc & & U^{(0)} \end{bmatrix} \in \mathbf{R}^{2^{n-1} \times 2^{n-2}}, \qquad U^{(0)} = \begin{bmatrix} u_0^0 & 0 \\ u_0^1 & 0 \\ 0 & u_0^2 \\ 0 & u_0^3 \end{bmatrix},$$

$$U_n^{(1)} = \begin{bmatrix} U^{(1)} & & & \bigcirc \\ & U^{(1)} & & \\ & & \ddots & \\ \bigcirc & & & U^{(1)} \end{bmatrix} \in \mathbf{R}^{2^{n-1}\times 2^{n-2}}, \qquad U^{(1)} = \begin{bmatrix} u_1^0 & 0 \\ u_1^1 & 0 \\ 0 & u_1^2 \\ 0 & u_1^3 \end{bmatrix},$$

$$U_n^{(2)} = \begin{bmatrix} U^{(2)} & & & \bigcirc \\ & U^{(2)} & & \\ & & \ddots & \\ \bigcirc & & & U^{(2)} \end{bmatrix} \in \mathbf{R}^{2^{n-1}\times 2^{n-2}}, \qquad U^{(2)} = \begin{bmatrix} u_2^0 & 0 \\ u_2^1 & 0 \\ 0 & u_2^2 \\ 0 & u_2^3 \end{bmatrix},$$

$$U_n^{(3)} = \begin{bmatrix} U^{(3)} & & & \bigcirc \\ & U^{(3)} & & \\ & & \ddots & \\ \bigcirc & & & U^{(3)} \end{bmatrix} \in \mathbf{R}^{2^{n-1}\times 2^{n-2}}, \qquad U^{(3)} = \begin{bmatrix} u_3^0 & 0 \\ u_3^1 & 0 \\ 0 & u_3^2 \\ 0 & u_3^3 \end{bmatrix},$$

which we shall denote by

$$U_n\left[\begin{pmatrix} u_0^0 & u_0^2 \\ u_0^1 & u_0^3 \end{pmatrix}; \begin{pmatrix} u_1^0 & u_1^2 \\ u_1^1 & u_1^3 \end{pmatrix}; \begin{pmatrix} u_2^0 & u_2^2 \\ u_2^1 & u_2^3 \end{pmatrix}; \begin{pmatrix} u_3^0 & u_3^2 \\ u_3^1 & u_3^3 \end{pmatrix}\right]$$

and abbreviate by U_n. The transfer matrix M_n is then equal to

$$U_n\left[\begin{pmatrix} a & a \\ b & b \end{pmatrix}; \begin{pmatrix} b & b \\ c & c \end{pmatrix}; \begin{pmatrix} a^{-1} & a^{-1} \\ b^{-1} & b^{-1} \end{pmatrix}; \begin{pmatrix} b^{-1} & b^{-1} \\ c^{-1} & c^{-1} \end{pmatrix}\right].$$

We shall denote the k^{th} column of U_n by u_k, $k = 0, 1, \ldots, 2^n - 1$.

Efficient processing with duodiagonal matrices U_n depends on the following *key* observations regarding their nonzero entries:

(a) the nonzero entries of u_k occur exactly at positions $2k \bmod 2^n$ and $(2k+1) \bmod 2^n$.

(b) the parameters u_j^{2i} and u_j^{2i+1} ($i = 0, 1$, $j = 0, 1, 2, 3$) are the nonzero entries of $u_{2^{n-2}j+2k+i}$, $0 \le k \le 2^{n-3} - 1$,

eg. for U_5, the parameters u_1^2 and u_1^3 (i.e. $i = 1$, $j = 1$) are the nonzero entries of u_9, u_{11}, u_{13} and u_{15}.

Equivalently, the parameters u_j^{2i} and u_j^{2i+1} are the nonzero entries of u_k, for those $k \in \{0, 1, \ldots, 2^n - 1\}$ where the leading bit pair of $\sigma_n(k)$ is $\sigma_2(j)$ and the trailing bit

of $\sigma_n(k)$ is $\sigma_1(i)$. In the above example, the only 5-bit strings with leading bit pair 01 and trailing bit 1 are

$$\sigma_5(9) = 01001,\ \ \sigma_5(11) = 01011,\ \ \sigma_5(13) = 01101 \text{ and } \sigma_5(15) = 01111.$$

Combining the above observations, we have:

Proposition 2.3.1 *For $i = 0, 1$, $j = 0, 1, 2, 3$, the parameter u_j^{2i} appears as the $(v(\omega), v(2\omega))$ entry of U_n where $\omega \in \{0,1\}^n$ satisfies $\omega(1) \circ \omega(2) = \sigma_2(j)$ and $\omega(n) = \sigma_1(i)$; the parameter u_j^{2i+1} appears as the $(v(\omega), v(2\omega + 1))$ entry of U_n for those same ω's.*

We remind the reader that for a string $\mu \in \{0,1\}^n$, $v(\mu)$ denotes the integer value it represents, and that for $i = 0, 1$, $j = 0, 1, 2, 3$, $\sigma_1(i)$ and $\sigma_2(j)$ denote the 1-bit binary representation of i and the 2-bit binary representation of j respectively (see Section 1.2).

Suppose $\mathbf{E} \subseteq \{0,1\}^n$ is such that all strings in $\mathbf{E}$ have the same leading bit pair and the same trailing bit. Recalling that a matrix-vector product is a linear combination of the columns of the matrix with coefficients given by the entries of the vector, we see that

$$U_n x_{\mathbf{E}} = \sum_{\substack{k \text{ where} \\ x_{\mathbf{E}}(k) = 1}} u_k = \sum_{\substack{k \text{ where} \\ \sigma_n(k) \in \mathbf{E}}} u_k.$$

From observation (b), the u_k's involved in the vector sum have the same two parameters u_j^{2i} and u_j^{2i+1} (for some i, j) as their nonzero entries, and applying observation (a) to each such u_k, we see that the nonzero entries of $U_n x_{\mathbf{E}}$ have indices in $v(2\mathbf{E}) \cup v(2\mathbf{E} + 1)$: u_j^{2i} appears at indices $v(2\mathbf{E})$ while u_j^{2i+1} appears at indices $v(2\mathbf{E} + 1)$. We have thus shown the following:

Theorem 2.3.2 *Let $\mathbf{E} \subseteq \{0,1\}^n$, $n \geq 3$, be such that all strings in $\mathbf{E}$ have the same leading bit pair and the same trailing bit. Then*

$$U_n x_{\mathbf{E}} = u_j^{2i} x_{2\mathbf{E}} + u_j^{2i+1} x_{2\mathbf{E}+1}$$

for some i, j.

Consider now applying U_n to the indicial vector $x_{\omega,k,t} \in \mathcal{S}_{n,l}$. Let $\mathbf{E} = \mathbf{I}_{\omega,k,t}$. Recall from Definition 2.5 that $\mathbf{E}^0 = \mathbf{I}^0_{\omega,k,t}$ and $\mathbf{E}^1 = \mathbf{I}^1_{\omega,k,t}$ ($\mathbf{E}^0$ and $\mathbf{E}^1$ could possibly be empty), and that $\mathbf{E}$ is the disjoint union of $\mathbf{E}^0$ and $\mathbf{E}^1$. By Proposition 2.1.5, $\mathbf{E}^0$ and $\mathbf{E}^1$

each contain strings with the same leading bit pair and the same trailing bit. Applying Therorem 2.3.2 to $\mathbf{E}^0$ and to $\mathbf{E}^1$, we have:

$$\begin{aligned} U_n x_{\mathbf{E}} &= U_n(x_{\mathbf{E}^0} + x_{\mathbf{E}^1}) \\ &= U_n x_{\mathbf{E}^0} + U_n x_{\mathbf{E}^1} \\ &= (u_j^{2i} x_{2\mathbf{E}^0} + u_j^{2i+1} x_{2\mathbf{E}^0+1}) + (u_{j'}^{2i'} x_{2\mathbf{E}^1} + u_{j'}^{2i'+1} x_{2\mathbf{E}^1+1}) \end{aligned}$$

for some $0 \leq i, i' \leq 1$ and $0 \leq j, j' \leq 3$ with $(i,j) \neq (i',j')$. By Theorem 2.1.8, $2\mathbf{E}^0$, $2\mathbf{E}^0+1$, $2\mathbf{E}^1$ and $2\mathbf{E}^1+1$ are themselves suffix-based indicial sets. Enumerating the possibilities, we have the following four cases for the formation of $U_n x_{\mathbf{E}}$:

Theorem 2.3.3 *Let $x_{\omega,k,t} \in \mathcal{S}_{n,l}$ and $\mathbf{E} = \mathbf{I}_{\omega,k,t}$. Then $U_n x_{\mathbf{E}}$ is a linear combination of (possibly zero) suffix-based indicial vectors as follows:*

(a) trailing bit of ω is 0 and t is even:

$$U_n x_{\mathbf{E}} = (u_0^0 x_{\omega o 0,k,t} + u_0^1 x_{\omega o 1,k+1,t+1}) + (u_1^0 x_{\omega o 0,k,t-1} + u_1^1 x_{\omega o 1,k+1,t})$$

(b) trailing bit of ω is 0 and t is odd:

$$U_n x_{\mathbf{E}} = (u_2^0 x_{\omega o 0,k-1,t-1} + u_2^1 x_{\omega o 1,k,t}) + (u_3^0 x_{\omega o 0,k-1,t} + u_3^1 x_{\omega o 1,k,t+1})$$

(c) trailing bit of ω is 1 and t is even:

$$U_n x_{\mathbf{E}} = (u_2^2 x_{\omega o 0,k-1,t} + u_2^3 x_{\omega o 1,k,t-1}) + (u_3^2 x_{\omega o 0,k-1,t+1} + u_3^3 x_{\omega o 1,k,t})$$

(d) trailing bit of ω is 1 and t is odd:

$$U_n x_{\mathbf{E}} = (u_0^2 x_{\omega o 0,k,t+1} + u_0^3 x_{\omega o 1,k+1,t}) + (u_1^2 x_{\omega o 0,k,t} + u_1^3 x_{\omega o 1,k+1,t-1})$$

As an illustration of Theorem 2.3.3, we work out the action of U_5 on some of the basis vectors in $\mathcal{S}_{5,1}$ in the example below. The columns of the 32×32 identity matrix I_5 will be denoted by $\{e_0, e_1, \ldots, e_{31}\}$. We urge the reader to go through the example carefully, and to observe in each case how the result of applying U_5 to an indicial vector could be expressed as a linear combination of 2 or 4 indicial vectors.

eg. (a) $\mathbf{I}^5_{0,1,2} = \{00010, 00100, 01000\}$, $x^5_{0,1,2} = e_2 + e_4 + e_8$,

$$\begin{aligned} U_5 x^5_{0,1,2} &= U_5 e_2 + U_5 e_4 + U_5 e_8 \\ &= u_2 + u_4 + u_8 \\ &= (u_0^0 e_4 + u_0^1 e_5) + (u_0^0 e_8 + u_0^1 e_9) + (u_1^0 e_{16} + u_1^1 e_{17}) \end{aligned}$$

$$= u_0^0(e_4 + e_8) + u_0^1(e_5 + e_9) + u_1^0 e_{16} + u_1^1 e_{17}$$

$$= u_0^0 x^5_{00,1,2} + u_0^1 x^5_{01,2,3} + u_1^0 x^5_{00,1,1} + u_1^1 x^5_{01,2,2}$$

(*b*) $\mathbf{I}^5_{0,2,3} = \{10010, 10100\}$, $x^5_{0,2,3} = e_{18} + e_{20}$,

$U_5 x^5_{0,2,3} = u_{18} + u_{20}$

$$= (u_2^0 e_4 + u_2^1 e_5) + (u_2^0 e_8 + u_2^1 e_9)$$

$$= u_2^0 x^5_{00,1,2} + u_2^1 x^5_{01,2,3}$$

(*c*) $\mathbf{I}^5_{1,4,2} = \{10111, 11011, 11101\}$, $x^5_{1,4,2} = e_{23} + e_{27} + e_{29}$,

$U_5 x^5_{1,4,2} = u_{23} + u_{27} + u_{29}$

$$= (u_2^2 e_{14} + u_2^3 e_{15}) + (u_3^2 e_{22} + u_3^3 e_{23}) + (u_3^2 e_{26} + u_3^3 e_{27})$$

$$= u_2^2 x^5_{10,3,2} + u_2^3 x^5_{11,4,1} + u_3^2 x^5_{10,3,3} + u_3^3 x^5_{11,4,2}$$

(*d*) $\mathbf{I}^5_{1,3,1} = \{00111\}$, $x^5_{1,3,1} = e_7$,

$U_5 x^5_{1,3,1} = u_7$

$$= u_0^2 e_{14} + u_0^3 e_{15}$$

$$= u_0^2 x^5_{10,3,2} + u_0^3 x^5_{11,4,1}$$

Returning to our analysis, we note that if $\mathbf{E}^0 = \emptyset$, then $x_{2\mathbf{E}^0} = x_{2\mathbf{E}^0+1} = 0$, and that if $\mathbf{E}^1 = \emptyset$, then $x_{2\mathbf{E}^1} = x_{2\mathbf{E}^1+1} = 0$. However, $\mathbf{E}^0$ and $\mathbf{E}^1$ cannot both be empty since $\mathbf{E} = \mathbf{E}^0 \cup \mathbf{E}^1$ and $\mathbf{E}$ is nonempty. In addition, the nonzero vectors among $x_{2\mathbf{E}^0}$, $x_{2\mathbf{E}^0+1}$, $x_{2\mathbf{E}^1}$ and $x_{2\mathbf{E}^1+1}$ are distinct from each other since $2\mathbf{E}^0$, $2\mathbf{E}^0 + 1$, $2\mathbf{E}^1$ and $2\mathbf{E}^1 + 1$ are pairwise disjoint by Proposition 2.1.6. *So $U_n x_{\mathbf{E}}$ is a linear combination of either 2 or 4 suffix-based indicial vectors.*

We can in fact relate $U_n x_{\mathbf{E}}$ to the vectors in the basis $\mathcal{S}_{n,l}$. Define a subvector of a vector x to be a vector obtained by setting zero or more entries of x to 0, i.e. a subvector has the same number of entries but more of them are 0; analogously, a subcolumn of a matrix A is a column obtained by setting zero or more entries of some column of A to 0. Recall that $\mathbf{E} = \mathbf{I}_{\omega,k,t}$, and $\omega \in \{0,1\}^l$. By Theorem 2.1.8, each of $2\mathbf{E}^0$ and $2\mathbf{E}^1$ is of the form $\mathbf{I}_{\omega\circ 0,k',t'}$ for some k' and t', and each of $2\mathbf{E}^0 + 1$ and $2\mathbf{E}^1 + 1$ is of the form $\mathbf{I}_{\omega\circ 1,k'',t''}$ for some k'' and t''. Now,

$$\omega \circ 0 = \omega(1) \circ (\omega(2) \circ \cdots \circ \omega(l) \circ 0) = \omega(1) \circ 2\omega,$$

and $$\omega \circ 1 = \omega(1) \circ (\omega(2) \circ \cdots \circ \omega(l) \circ 1) = \omega(1) \circ (2\omega + 1).$$

Therefore $\mathbf{I}_{\omega o 0,k',t'} \subseteq \mathbf{I}_{2\omega,k',t'}$ and $\mathbf{I}_{\omega o 1,k'',t''} \subseteq \mathbf{I}_{2\omega+1,k'',t''}$ since 2ω and $2\omega+1$ are suffixes of $\omega \circ 0$ and $\omega \circ 1$ respectively. It follows then that $x_{2\mathbf{E}^0}$, $x_{2\mathbf{E}^0+1}$, $x_{2\mathbf{E}^1}$ and $x_{2\mathbf{E}^1+1}$ are subvectors of vectors in $\mathcal{S}_{n,l}$ since $|2\omega| = |2\omega+1| = l$. Thus $U_n x_{\mathbf{E}}$ is a linear combination of either 2 or 4 subvectors in $\mathcal{S}_{n,l}$ (with each subvector arising from a different vector in $\mathcal{S}_{n,l}$).

2.4 Structure of the column and row projection matrices

Armed with our understanding of the action of duodiagonal matrices on suffix-based indicial bases, the analysis of the structure of the column projection matrix $P^C_{n,l}$ becomes straightforward. We shall show that for $l \geq 1$, $P^C_{n,l}$ is *sparse* with either 2 or 4 nonzero entries per column, and we shall precisely locate the positions of those entries, and express their values in a way that enables them to be computed without using vectors in $\mathbf{R}^{2^n}$. By exploiting an important relationship between suffix-based and prefix-based indicial objects, we shall show that the row projection matrix $P^R_{n,l}$ has the same sparsity structure as the corresponding column projection matrix $P^C_{n,l}$.

Recall that $P^C_{n,l} = D_X^{-1} X^* M_n X$, where the columns of X are the vectors in $\mathcal{S}_{n,l}$ and $D_X = X^*X$. We index the rows and columns of $P^C_{n,l}$ by the triple (ω,k,t) where $x_{\omega,k,t}$ is a column of X. Then the entry in row (ω',k',t') and column (ω,k,t) of $P^C_{n,l}$ is given by:

$$\frac{1}{\|x_{\omega',k',t'}\|^2}\langle x_{\omega',k',t'}, M_n x_{\omega,k,t}\rangle \;=\; \frac{1}{|\mathbf{I}_{\omega',k',t'}|}\langle x_{\omega',k',t'}, M_n x_{\omega,k,t}\rangle.$$

Recall that

$$M_n = U_n \left[\begin{pmatrix} a & a \\ b & b \end{pmatrix}; \begin{pmatrix} b & b \\ c & c \end{pmatrix}; \begin{pmatrix} a^{-1} & a^{-1} \\ b^{-1} & b^{-1} \end{pmatrix}; \begin{pmatrix} b^{-1} & b^{-1} \\ c^{-1} & c^{-1} \end{pmatrix} \right].$$

Let $\mathbf{E} = \mathbf{I}_{\omega,k,t}$. The analysis of Section 2.3 applied to M_n shows that $M_n x_{\mathbf{E}}$ is a linear combination of either 2 or 4 subcolumns of X (with each subcolumn arising from a different column of X). Since the columns of X have pairwise disjoint supports (cf. Proposition 2.1.2), $P^C_{n,l}$ is sparse with 2 or 4 nonzero entries per column arising from the nonzero inner products $\langle x_{\omega',k',t'}, M_n x_{\mathbf{E}}\rangle$. Specifically, column (ω,k,t) of $P^C_{n,l}$ has 2 nonzero entries if one of $\mathbf{E}^0$ and $\mathbf{E}^1$ is empty, and has 4 nonzero entries if both $\mathbf{E}^0$ and $\mathbf{E}^1$ are nonempty. For completeness, we enumerate the possible nonzero inner products (cf. Theorem 2.3.3). The reader who is not interested in the details may wish to skip the enumeration.

(a) trailing bit of ω is 0 and t is even:

$$\begin{aligned}
\langle x_{2\omega,k,t}, M_n x_{\mathbf{E}} \rangle &= \langle x_{2\omega,k,t}, u_0^0 x_{\omega o 0,k,t} \rangle \\
&= u_0^0 \|x_{\omega o 0,k,t}\|^2 \\
&= u_0^0 |\mathbf{I}_{\omega o 0,k,t}| \\
&= a|\mathbf{I}_{\omega o 0,k,t}| \\
&= a|2\mathbf{E}^0| \\
&= a|\mathbf{E}^0| \quad \text{by Theorem 2.1.7.}
\end{aligned}$$

Similarly,

$$\langle x_{2\omega+1,k+1,t+1}, M_n x_{\mathbf{E}} \rangle = u_0^1 |\mathbf{I}_{\omega o 1,k+1,t+1}| = b|\mathbf{I}_{\omega o 1,k+1,t+1}| = b|\mathbf{E}^0|$$

$$\langle x_{2\omega,k,t-1}, M_n x_{\mathbf{E}} \rangle = u_1^0 |\mathbf{I}_{\omega o 0,k,t-1}| = b|\mathbf{I}_{\omega o 0,k,t-1}| = b|\mathbf{E}^1|$$

$$\langle x_{2\omega+1,k+1,t}, M_n x_{\mathbf{E}} \rangle = u_1^1 |\mathbf{I}_{\omega o 1,k+1,t}| = c|\mathbf{I}_{\omega o 1,k+1,t}| = c|\mathbf{E}^1|$$

(b) trailing bit of ω is 0 and t is odd:

$$\langle x_{2\omega,k-1,t-1}, M_n x_{\mathbf{E}} \rangle = u_2^0 |\mathbf{I}_{\omega o 0,k-1,t-1}| = a^{-1}|\mathbf{I}_{\omega o 0,k-1,t-1}| = a^{-1}|\mathbf{E}^0|$$

$$\langle x_{2\omega+1,k,t}, M_n x_{\mathbf{E}} \rangle = u_2^1 |\mathbf{I}_{\omega o 1,k,t}| = b^{-1}|\mathbf{I}_{\omega o 1,k,t}| = b^{-1}|\mathbf{E}^0|$$

$$\langle x_{2\omega,k-1,t}, M_n x_{\mathbf{E}} \rangle = u_3^0 |\mathbf{I}_{\omega o 0,k-1,t}| = b^{-1}|\mathbf{I}_{\omega o 0,k-1,t}| = b^{-1}|\mathbf{E}^1|$$

$$\langle x_{2\omega+1,k,t+1}, M_n x_{\mathbf{E}} \rangle = u_3^1 |\mathbf{I}_{\omega o 1,k,t+1}| = c^{-1}|\mathbf{I}_{\omega o 1,k,t+1}| = c^{-1}|\mathbf{E}^1|$$

(c) trailing bit of ω is 1 and t is even:

$$\langle x_{2\omega,k-1,t}, M_n x_{\mathbf{E}} \rangle = u_2^2 |\mathbf{I}_{\omega o 0,k-1,t}| = a^{-1}|\mathbf{I}_{\omega o 0,k-1,t}| = a^{-1}|\mathbf{E}^0|$$

$$\langle x_{2\omega+1,k,t-1}, M_n x_{\mathbf{E}} \rangle = u_2^3 |\mathbf{I}_{\omega o 1,k,t-1}| = b^{-1}|\mathbf{I}_{\omega o 1,k,t-1}| = b^{-1}|\mathbf{E}^0|$$

$$\langle x_{2\omega,k-1,t+1}, M_n x_{\mathbf{E}} \rangle = u_3^2 |\mathbf{I}_{\omega o 0,k-1,t+1}| = b^{-1}|\mathbf{I}_{\omega o 0,k-1,t+1}| = b^{-1}|\mathbf{E}^1|$$

$$\langle x_{2\omega+1,k,t}, M_n x_{\mathbf{E}} \rangle = u_3^3 |\mathbf{I}_{\omega o 1,k,t}| = c^{-1}|\mathbf{I}_{\omega o 1,k,t}| = c^{-1}|\mathbf{E}^1|$$

(d) trailing bit of ω is 1 and t is odd:

$$\langle x_{2\omega,k,t+1}, M_n x_{\mathbf{E}} \rangle = u_0^2 |\mathbf{I}_{\omega o 0,k,t+1}| = a|\mathbf{I}_{\omega o 0,k,t+1}| = a|\mathbf{E}^0|$$

$$\langle x_{2\omega+1,k+1,t}, M_n x_{\mathbf{E}} \rangle = u_0^3 |\mathbf{I}_{\omega o 1,k+1,t}| = b|\mathbf{I}_{\omega o 1,k+1,t}| = b|\mathbf{E}^0|$$

$$\langle x_{2\omega,k,t}, M_n x_{\mathbf{E}} \rangle = u_1^2 |\mathbf{I}_{\omega o 0,k,t}| = b|\mathbf{I}_{\omega o 0,k,t}| = b|\mathbf{E}^1|$$

$$\langle x_{2\omega+1,k+1,t-1}, M_n x_{\mathbf{E}} \rangle = u_1^3 |\mathbf{I}_{\omega o 1,k+1,t-1}| = c|\mathbf{I}_{\omega o 1,k+1,t-1}| = c|\mathbf{E}^1|$$

Note that in the above enumeration, we could state precisely the possible nonzero inner products, and thus we can precisely locate the positions of the nonzero entries of $P^C_{n,l}$. More importantly, each inner product (involving two vectors in $\mathbf{R}^{2^n}$) was expressed as a product of an entry in M_n and the cardinality of a suffix-based indicial set. In Chapter 3, we shall develop formulas for finding those cardinalities. *Thus the projection matrix $P^C_{n,l}$ can be computed in time proportional to $|\mathcal{S}_{n,l}|$ and without using any vectors in $\mathbf{R}^{2^n}$.*

The analysis of the structure of the column projection matrix $P^C_{n,l}$ could be adapted to the row projection matrix $P^R_{n,l} = D_Y^{-1}Y^*M_n^*Y$ by considering directly how multiplication by M_n^* affects prefix-based indicial vectors. It is, however, more illuminating to exploit the relationship between suffix-based and prefix-based indicial vectors.

Consider the binary reversal matrix $\tilde{R}_n \in \mathbf{R}^{2^n \times 2^n}$, whose only nonzero entries are ones in row i and column j, where the n-bit binary representation of i and j are the reversal of each other, i.e.

$$(\tilde{R}_n)_{i,j} = \begin{cases} 1 & \text{if } \sigma_n(i) = (\sigma_n(j))^R \\ 0 & \text{otherwise} \end{cases} \qquad 0 \le i,j \le 2^n - 1.$$

$\tilde{R}_n$ is a *reflection*: it is symmetric, involutary ($\tilde{R}_n^2 = I_n$) and orthogonal ($\tilde{R}_n^*\tilde{R}_n = \tilde{R}_n^2 = I_n$). If $e_j \in \mathbf{R}^{2^n}$ is the j^{th} column of the identity matrix I_n, then $\tilde{R}_n e_j = e_{\tilde{j}}$ where we write $v((\sigma_n(j))^R)$ as $\tilde{j}$. Therefore for the suffix-based indicial vector $x_{\omega,k,t}$, we have $\tilde{R}_n x_{\omega,k,t} = y_{\omega^R,k,t}$ since $\tilde{R}_n$ does not change the 1-bit count and bit transition count of an n-bit string. We thus have a one-to-one correspondence between suffix-based indicial vectors in $\mathcal{S}_{n,l}$ and prefix-based indicial vectors in $\mathcal{T}_{n,l}$, and $\tilde{R}_n\mathcal{S}_{n,l} = \{\tilde{R}_n x : x \in \mathcal{S}_{n,l}\} = \mathcal{T}_{n,l}$. By a suitable arrangement of the columns of Y, we can make $Y = \tilde{R}_n X$. Then

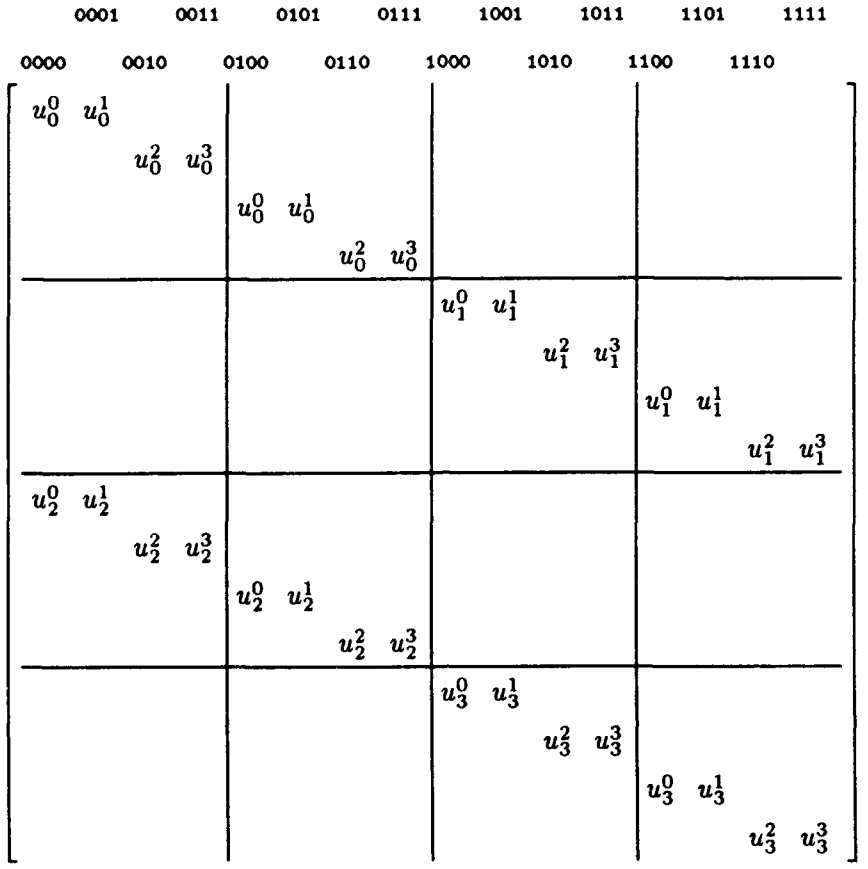
$$P^R_{n,l} = D_Y^{-1}Y^*M_n^*Y = D_X^{-1}(X^*\tilde{R}_n^*)M_n^*(\tilde{R}_nX) = D_X^{-1}X^*(\tilde{R}_nM_n^*\tilde{R}_n)X$$

since

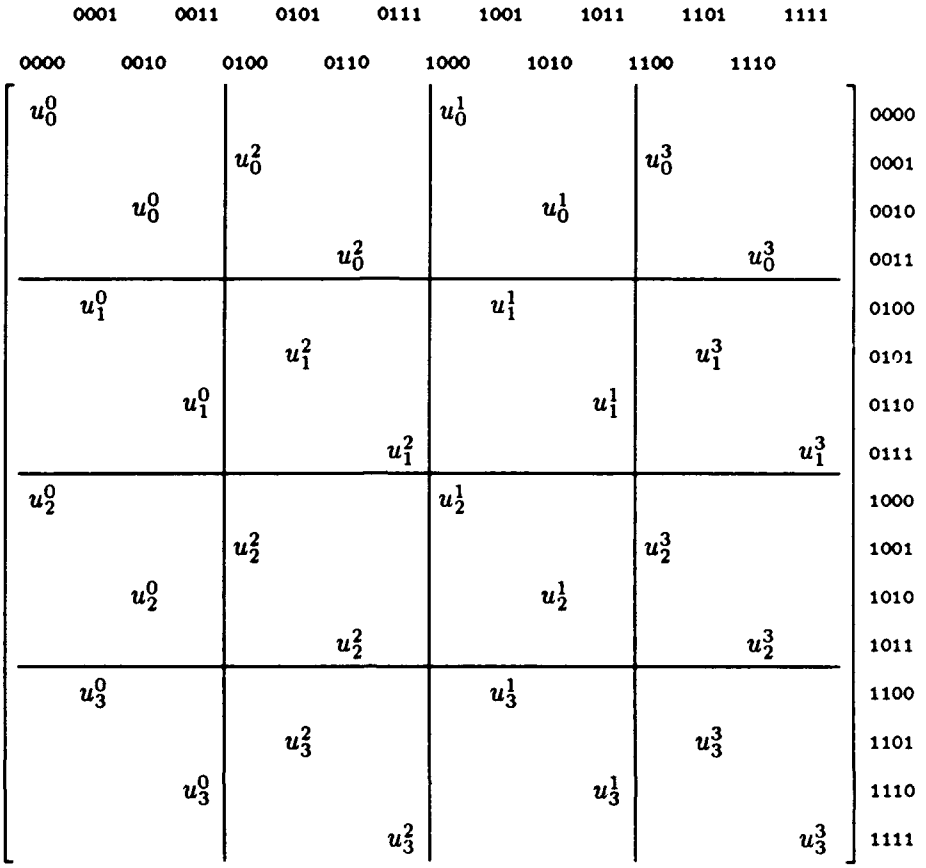
$$D_Y = Y^*Y = (X^*\tilde{R}_n^*)(\tilde{R}_nX) = X^*(\tilde{R}_n^*\tilde{R}_n)X = X^*X = D_X.$$

The sparsity structure of $\tilde{R}_nM_n^*\tilde{R}_n$ is identical to that of M_n (the parameter values permute), as Theorem 2.4.1 shows. We illustrate it for $n = 4$. Note that for a matrix $B \in \mathbf{R}^{2^n \times 2^n}$, $B\tilde{R}_n$ is a permutation of the columns of B with columns i and j interchanged if $i = \tilde{j}$ $(0 \le i,j \le 2^n - 1)$, while $\tilde{R}_nB$ is a permutation of the rows of B arising from the same interchange of rows. In particular, the remarks hold for $U_4^*\tilde{R}_4$ and $\tilde{R}_4(U_4^*\tilde{R}_4)$ respectively.

$$U_4^* =$$


0001 0011 0101 0111 1001 1011 1101 1111
0000 0010 0100 0110 1000 1010 1100 1110
u_0^0 u_0^1
u_0^2 u_0^3
u_0^0 u_0^1
u_0^2 u_0^3
u_1^0 u_1^1
u_1^2 u_1^3
u_1^0 u_1^1
u_1^2 u_1^3
u_2^0 u_2^1
u_2^2 u_2^3
u_2^0 u_2^1
u_2^2 u_2^3
u_3^0 u_3^1
u_3^2 u_3^3
u_3^0 u_3^1
u_3^2 u_3^3

$$U_4^* \tilde{R}_4 =$$


0001 0011 0101 0111 1001 1011 1101 1111
0000 0010 0100 0110 1000 1010 1100 1110
u_0^0 u_0^1
u_0^2 u_0^3
u_0^0 u_0^1
u_0^2 u_0^3
u_1^0 u_1^1
u_1^2 u_1^3
u_1^0 u_1^1
u_1^2 u_1^3
u_2^0 u_2^1
u_2^2 u_2^3
u_2^0 u_2^1
u_2^2 u_2^3
u_3^0 u_3^1
u_3^2 u_3^3
u_3^0 u_3^1
u_3^2 u_3^3
0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

$$\tilde{R}_4(U_4^*\tilde{R}_4) = \left[\begin{array}{cccc|cccc|cccc|l}
u_0^0 & & & & u_0^1 & & & & & & & & 0000 \\
u_2^0 & & & & u_2^1 & & & & & & & & 0001 \\
 & u_1^0 & & & & u_1^1 & & & & & & & 0010 \\
 & u_3^0 & & & & u_3^1 & & & & & & & 0011 \\
\hline
 & & u_0^0 & & & & u_0^1 & & & & & & 0100 \\
 & & u_2^0 & & & & u_2^1 & & & & & & 0101 \\
 & & & u_1^0 & & & & u_1^1 & & & & & 0110 \\
 & & & u_3^0 & & & & u_3^1 & & & & & 0111 \\
\hline
 & & & & u_0^2 & & & & u_0^3 & & & & 1000 \\
 & & & & u_2^2 & & & & u_2^3 & & & & 1001 \\
 & & & & & u_1^2 & & & & u_1^3 & & & 1010 \\
 & & & & & u_3^2 & & & & u_3^3 & & & 1011 \\
\hline
 & & & & & & u_0^2 & & & & u_0^3 & & 1100 \\
 & & & & & & u_2^2 & & & & u_2^3 & & 1101 \\
 & & & & & & & u_1^2 & & & & u_1^3 & 1110 \\
 & & & & & & & u_3^2 & & & & u_3^3 & 1111
\end{array}\right]$$

$$= U_4\left[\begin{pmatrix} u_0^0 & u_1^0 \\ u_2^0 & u_3^0 \end{pmatrix}; \begin{pmatrix} u_0^2 & u_1^2 \\ u_2^2 & u_3^2 \end{pmatrix}; \begin{pmatrix} u_0^1 & u_1^1 \\ u_2^1 & u_3^1 \end{pmatrix}; \begin{pmatrix} u_0^3 & u_1^3 \\ u_2^3 & u_3^3 \end{pmatrix}\right].$$

Theorem 2.4.1 $\tilde{R}_n U_n^*\left[\begin{pmatrix} u_0^0 & u_0^2 \\ u_0^1 & u_0^3 \end{pmatrix}; \begin{pmatrix} u_1^0 & u_1^2 \\ u_1^1 & u_1^3 \end{pmatrix}; \begin{pmatrix} u_2^0 & u_2^2 \\ u_2^1 & u_2^3 \end{pmatrix}; \begin{pmatrix} u_3^0 & u_3^2 \\ u_3^1 & u_3^3 \end{pmatrix}\right]\tilde{R}_n =$

$U_n\left[\begin{pmatrix} u_0^0 & u_1^0 \\ u_2^0 & u_3^0 \end{pmatrix}; \begin{pmatrix} u_0^2 & u_1^2 \\ u_2^2 & u_3^2 \end{pmatrix}; \begin{pmatrix} u_0^1 & u_1^1 \\ u_2^1 & u_3^1 \end{pmatrix}; \begin{pmatrix} u_0^3 & u_1^3 \\ u_2^3 & u_3^3 \end{pmatrix}\right]$.

Proof. Abbreviate $U_n\left[\begin{pmatrix} u_0^0 & u_0^2 \\ u_0^1 & u_0^3 \end{pmatrix}; \begin{pmatrix} u_1^0 & u_1^2 \\ u_1^1 & u_1^3 \end{pmatrix}; \begin{pmatrix} u_2^0 & u_2^2 \\ u_2^1 & u_2^3 \end{pmatrix}; \begin{pmatrix} u_3^0 & u_3^2 \\ u_3^1 & u_3^3 \end{pmatrix}\right]$ by U_n. We shall determine where the nonzero entries of $\tilde{R}_n U_n^* \tilde{R}_n$ are. It is easily verified that the (i,j) entry of U_n appears as the $(\bar{j},\bar{i})$ entry of $\tilde{R}_n U_n^* \tilde{R}_n$, or in terms of strings, the $(v(\mu), v(\omega))$ entry of U_n appears as the $(v(\omega^R), v(\mu^R))$ entry of $\tilde{R}_n U_n^* \tilde{R}_n$ for $\mu, \omega \in \{0,1\}^n$. In particular, for $\omega \in \{0,1\}^n$, the $(v(\omega), v(2\omega))$ and $(v(\omega), v(2\omega+1))$ entries of U_n appear respectively as the $(v((2\omega)^R), v(\omega^R))$ and $(v((2\omega+1)^R), v(\omega^R))$ entries of $\tilde{R}_n U_n^* \tilde{R}_n$.

Consider the parameter u_2^2. From Proposition 2.3.1, u_2^2 appears as the $(v(\omega), v(2\omega))$

entry of U_n where $\omega \in \{0,1\}^n$ satisfies $\omega(1) \circ \omega(2) = 10$ and $\omega(n) = 1$. Let

$$\begin{aligned} A &= \{\omega \in \{0,1\}^n : \omega(1) \circ \omega(2) = 10,\ \omega(n) = 1\}, \\ \text{and} \quad B &= \{\omega' \in \{0,1\}^n : \omega'(1) \circ \omega'(2) = 01,\ \omega'(n) = 0\}. \end{aligned}$$

We claim that

$$\{((2\omega)^R, \omega^R) : \omega \in A\} = \{(\omega', 2\omega' + 1) : \omega' \in B\}. \tag{2.2}$$

Note that $|A| = |B| = 2^{n-3}$, and that for each set in equation (2.2), each pair in it can arise from only one string in A (or B). It thus suffices to show that for $\omega \in A$, $((2\omega)^R, \omega^R) = (\omega', 2\omega' + 1)$ for some $\omega' \in B$.

Let $\omega \in A$, and $\omega' = (2\omega)^R$. Then $\omega(1) = 1$, $\omega(2) = 0$, and $\omega(n) = 1$. In addition,

$$\begin{aligned} \omega' &= [\omega(2) \circ \cdots \circ \omega(n) \circ 0]^R \\ &= 0 \circ \omega(n) \circ \cdots \circ \omega(2), \\ \text{and} \quad 2\omega' + 1 &= \omega(n) \circ \omega(n-1) \circ \cdots \circ \omega(2) \circ 1 \\ &= \omega^R. \end{aligned}$$

So $((2\omega)^R, \omega^R) = (\omega', 2\omega' + 1)$, and $\omega'(1) \circ \omega'(2) = 01$ and $\omega'(n) = 0$, i.e. $\omega' \in B$.

Thus

$$\{((2\omega)^R, \omega^R) : \omega \in A\} = \{(\omega', 2\omega' + 1) : \omega' \in B\},$$

and u_2^2 appears as the $(v(\omega'), v(2\omega' + 1)$ entry of $\tilde{R}_n U_n^* \tilde{R}_n$ where $\omega' \in \{0,1\}^n$ satisfies $\omega'(1) \circ \omega'(2) = 01$ and $\omega'(n) = 0$. By similarly considering the other fifteen parameters, we can characterize their positions in $\tilde{R}_n U_n^* \tilde{R}_n$ in the same manner. It then follows by applying Proposition 2.3.1 to $\tilde{R}_n U_n^* \tilde{R}_n$ that

$$\tilde{R}_n U_n^* \tilde{R}_n = U_n \left[\begin{pmatrix} u_0^0 & u_1^0 \\ u_2^0 & u_3^0 \end{pmatrix} ; \begin{pmatrix} u_0^2 & u_1^2 \\ u_2^2 & u_3^2 \end{pmatrix} ; \begin{pmatrix} u_0^1 & u_1^1 \\ u_2^1 & u_3^1 \end{pmatrix} ; \begin{pmatrix} u_0^3 & u_1^3 \\ u_2^3 & u_3^3 \end{pmatrix} \right]. \quad \square$$

Applying the above theorem to $\tilde{R}_n M_n^* \tilde{R}_n$, we have

$$\begin{aligned} \tilde{R}_n M_n^* \tilde{R}_n &= \tilde{R}_n U_n^* \left[\begin{pmatrix} a & a \\ b & b \end{pmatrix} ; \begin{pmatrix} b & b \\ c & c \end{pmatrix} ; \begin{pmatrix} a^{-1} & a^{-1} \\ b^{-1} & b^{-1} \end{pmatrix} ; \begin{pmatrix} b^{-1} & b^{-1} \\ c^{-1} & c^{-1} \end{pmatrix} \right] \tilde{R}_n \\ &= U_n \left[\begin{pmatrix} a & b \\ a^{-1} & b^{-1} \end{pmatrix} ; \begin{pmatrix} a & b \\ a^{-1} & b^{-1} \end{pmatrix} ; \begin{pmatrix} b & c \\ b^{-1} & c^{-1} \end{pmatrix} ; \begin{pmatrix} b & c \\ b^{-1} & c^{-1} \end{pmatrix} \right]. \end{aligned}$$

and so $P_{n,l}^R$ has the same structure as $P_{n,l}^C$.

2.5 Degenerate column and row projection matrices

For $l = 0$ and fixed n, the column and row projection matrices, $P^C_{n,l} = D_X^{-1} X^* M_n X$ and $P^R_{n,l} = D_X^{-1} X^* (\tilde{R}_n M_n^* \tilde{R}_n) X$ respectively, are degenerate in that they do not possess the sparsity structure present when $l \geq 1$. Instead, $P^C_{n,0}$ and $P^R_{n,0}$ have either 2, 4, 6 or 8 nonzero entries per column.

Since no suffixes are involved when $l = 0$, we index the rows and columns of $P^C_{n,0}$ by the pair (k,t), where $x_{\epsilon,k,t}$ is a column of X. The entry in row (k',t') and column (k,t) of $P^C_{n,0}$ is then given by

$$\frac{1}{\|x_{\epsilon,k',t'}\|^2} \langle x_{\epsilon,k',t'}, M_n x_{\epsilon,k,t} \rangle.$$

Let $\mathbf{E} = \mathbf{I}_{\epsilon,k,t}$. Then $\mathbf{E}^0 = \mathbf{I}^0_{\epsilon,k,t}$ and $\mathbf{E}^1 = \mathbf{I}^1_{\epsilon,k,t}$. Unlike the case $l \geq 1$, $\mathbf{E}^0$ and $\mathbf{E}^1$ each do not necessarily contain strings with the same leading bit pair and the same trailing bit as the suffixes are not specified. However, we can partition them according to the trailing bit of strings in them:

$$\mathbf{E}^0 = \mathbf{E}^0_0 \cup \mathbf{E}^0_1, \qquad \mathbf{E}^1 = \mathbf{E}^1_0 \cup \mathbf{E}^1_1,$$

where

$$\mathbf{E}^0_0 = \mathbf{I}^0_{0,k,t}, \ \mathbf{E}^0_1 = \mathbf{I}^0_{1,k,t}, \quad \text{and} \quad \mathbf{E}^1_0 = \mathbf{I}^1_{0,k,t}, \ \mathbf{E}^1_1 = \mathbf{I}^1_{1,k,t}.$$

$\mathbf{E}^0_0$, $\mathbf{E}^0_1$, $\mathbf{E}^1_0$, $\mathbf{E}^1_1$ are pairwise disjoint by definition, and by Proposition 2.1.5, they each contain strings with the same leading bit pair and the same trailing bit. By Theorem 2.1.8, each of $2\mathbf{E}^0_0$, $2\mathbf{E}^0_0 + 1$, ..., $2\mathbf{E}^1_1$ and $2\mathbf{E}^1_1 + 1$ are suffix-based indicial sets, and they are pairwise disjoint since:

(a) by Proposition 2.1.6,

  (i) $2\mathbf{E}^0_0$, $2\mathbf{E}^0_0 + 1$, $2\mathbf{E}^1_0$ and $2\mathbf{E}^1_0 + 1$ are pairwise disjoint

  (ii) $2\mathbf{E}^0_1$, $2\mathbf{E}^0_1 + 1$, $2\mathbf{E}^1_1$ and $2\mathbf{E}^1_1 + 1$ are pairwise disjoint

(b) a string μ from a set in case (i) has $\mu(n-1) = 0$ whereas a string μ from a set in ase (ii) has $\mu(n-1) = 1$.

Applying Theorem 2.3.2 to each of $\mathbf{E}^0_0$, $\mathbf{E}^0_1$, $\mathbf{E}^1_0$ and $\mathbf{E}^1_1$, we have

$$M_n x_{\mathbf{E}} = M_n x_{\mathbf{E}^0_0} + M_n x_{\mathbf{E}^0_1} + M_n x_{\mathbf{E}^1_0} + M_n x_{\mathbf{E}^1_1}$$

$$= (m_{000}x_{2\mathbf{E}_0^0} + m_{001}x_{2\mathbf{E}_0^0+1}) + (m_{010}x_{2\mathbf{E}_1^0} + m_{011}x_{2\mathbf{E}_1^0+1})$$
$$+(m_{100}x_{2\mathbf{E}_0^1} + m_{101}x_{2\mathbf{E}_0^1+1}) + (m_{110}x_{2\mathbf{E}_1^1} + m_{111}x_{2\mathbf{E}_1^1+1}).$$

for some parameters $m_{000}, \ldots, m_{111}$ of M_n. As before, we note that if $\mathbf{E}_0^0 = \emptyset$, then $x_{2\mathbf{E}_0^0} = x_{2\mathbf{E}_0^0+1} = 0$, and similarly for $\mathbf{E}_1^0$, $\mathbf{E}_0^1$ and $\mathbf{E}_1^1$. However, $\mathbf{E}_0^0$, $\mathbf{E}_1^0$, $\mathbf{E}_0^1$, $\mathbf{E}_1^1$ cannot all be empty since $\mathbf{E} = \mathbf{E}_0^0 \cup \mathbf{E}_1^0 \cup \mathbf{E}_0^1 \cup \mathbf{E}_1^1$ and $\mathbf{E}$ is nonempty. In addition, the nonzero vectors among $x_{2\mathbf{E}_0^0}, \ldots, x_{2\mathbf{E}_1^1+1}$ have pairwise disjoint supports. So $M_n x_{\mathbf{E}}$ is a linear combination of either 2, 4, 6 or 8 suffix-based indicial vectors. The four possibilities can actually occur, as the following example shows:

eg. (i) $\mathbf{E} = \mathbf{I}^4_{\epsilon,0,0} = \{0000\}$, $\mathbf{E}_0^0 = \{0000\}$, $\mathbf{E}_1^0 = \mathbf{E}_0^1 = \mathbf{E}_1^1 = \emptyset$.

(ii) $\mathbf{E} = \mathbf{I}^4_{\epsilon,1,1} = \{0001, 1000\}$, $\mathbf{E}_0^0 = \{1000\}$, $\mathbf{E}_1^0 = \{0001\}$, $\mathbf{E}_0^1 = \mathbf{E}_1^1 = \emptyset$.

(iii) $\mathbf{E} = \mathbf{I}^5_{\epsilon,2,3} = \{00101, 01001, 10010, 10100\}$,
$\mathbf{E}_0^0 = \{10010, 10100\}$, $\mathbf{E}_1^0 = \{00101\}$, $\mathbf{E}_0^1 = \emptyset$, $\mathbf{E}_1^1 = \{01001\}$.

(iv) $\mathbf{E} = \mathbf{I}^6_{\epsilon,3,2} = \{001110, 011100, 100011, 110001\}$,
$\mathbf{E}_0^0 = \{0C1110\}$, $\mathbf{E}_1^0 = \{100011\}$, $\mathbf{E}_0^1 = \{011100\}$, $\mathbf{E}_1^1 = \{110001\}$.

Thus $P^C_{n,0}$ has either 2, 4, 6 or 8 nonzero entries per column. Since $\tilde{R}_n M_n^* \tilde{R}_n$ has the same structure as M_n, the same conclusion holds for $P^R_{n,0}$.

2.6 Action of the transfer matrix on general indicial bases

The careful reader would no doubt question our choice of indicial sets. In particular, the exclusive use of the prefix or the suffix as one of the three parameters in our indicial functions might seem overly restrictive. In this section, we introduce a more general class of indicial sets, and consider how the transfer matrix acts on the corresponding indicial bases. We will then be able to justify our choice of approximating subspaces in Section 2.7.

Let $n \geq 1$, $0 \leq k \leq n$, $0 \leq t \leq n-1$ and $\omega_1, \omega_2 \in \{0,1\}^*$ with $0 \leq |\omega_1| + |\omega_2| \leq n$. Recall that for a string $\mu \in \{0,1\}^n$, $\kappa(\mu)$ and $\tau(\mu)$ denote its 1-bit count and bit transition count respectively. We define a general indicial set to be

$$\mathbf{G}^n_{\omega_1,\omega_2,k,t} := \{\mu \in \{0,1\}^n : \kappa(\mu) = k,\ \tau(\mu) = t,\ \omega_1 \text{ is a prefix of } \mu \text{ and } \omega_2 \text{ is a suffix of } \mu\}$$

and in analogous fashion to suffix-based indicial sets, we can define general indicial vectors

$z^n_{\omega_1,\omega_2,k,t}$ and general indicial bases $\mathcal{V}_{n,l_1,l_2}$, with $0 \le l_1 + l_2 \le n$. We will assume that n is a fixed integer ≥ 3, and omit it in writing indicial sets and vectors.

It is clear that suffix-based and prefix-based indicial objects are special cases of general indicial objects. Indeed, we have:

$$\mathbf{I}_{\omega,k,t} = \mathbf{G}_{\epsilon,\omega,k,t}, \quad x_{\omega,k,t} = z_{\epsilon,\omega,k,t}, \quad \mathcal{S}_{n,l} = \mathcal{V}_{n,0,l},$$

$$\text{and} \quad \mathbf{J}_{\omega,k,t} = \mathbf{G}_{\omega,\epsilon,k,t}, \quad y_{\omega,k,t} = z_{\omega,\epsilon,k,t}, \quad \mathcal{T}_{n,l} = \mathcal{V}_{n,l,0}.$$

In addition, since the leading (trailing) bit of a string can be determined from its trailing (leading) bit together with the parity of its bit-transition count (cf. Proposition 2.1.3), we have for nonempty general indicial sets $\mathbf{G}_{\omega_1,\omega_2,k,t}$ the following:

$$\mathbf{G}_{\omega_1,\omega_2,k,t} = \mathbf{G}_{\epsilon,\omega_2,k,t} \quad \text{if } |\omega_1| = 1 \text{ and } \omega_2 \ne \epsilon,$$

$$\text{and} \quad \mathbf{G}_{\omega_1,\omega_2,k,t} = \mathbf{G}_{\omega_1,\epsilon,k,t} \quad \text{if } |\omega_2| = 1 \text{ and } \omega_1 \ne \epsilon.$$

Therefore, $\mathcal{S}_{n,l} = \mathcal{V}_{n,0,l} = \mathcal{V}_{n,1,l}$ and $\mathcal{T}_{n,l} = \mathcal{V}_{n,l,0} = \mathcal{V}_{n,l,1}$.

We note that by the same type of proof as in Theorem 2.1.8, we can show that:

Theorem 2.6.1 *Let* $\mathbf{E} = \mathbf{G}^n_{\omega_1,\omega_2,k,t}$, $n \ge 3$, $|\omega_1| \ge 2$ *and* $|\omega_1| + |\omega_2| \le n$. *Then* $2\mathbf{E} = \mathbf{G}^n_{\omega_1',\omega_2',k',t'}$ *and* $2\mathbf{E}+1 = \mathbf{G}^n_{\omega_1'',\omega_2'',k'',t''}$ *for some* $\omega_1', \omega_2', k', t', \omega_1'', \omega_2'', k'', t''$ *with* $|\omega_1'| = |\omega_1''| = |\omega_1| - 1$ *and* $|\omega_2'| = |\omega_2''| = |\omega_2| + 1$. *Thus* $x_{2\mathbf{E}}$ *and* $x_{2\mathbf{E}+1}$ *belong to the basis* $\mathcal{V}_{n,|\omega_1|-1,|\omega_2|+1}$.

Consider now the action of M_n on a general indicial basis $\mathcal{V}_{n,l_1,l_2}$, $n \ge 3$, $l_1 \ge 2$ and $l_1 + l_2 \le n$. As usual, we work with the general duodiagonal matrix U_n instead of M_n.

Theorem 2.6.2 *Let* $n \ge 3$, $l_1 \ge 2$ *and* $l_1 + l_2 \le n$. *Then*

$$U_n \text{span}(\mathcal{V}_{n,l_1,l_2}) \subseteq \text{span}(\mathcal{V}_{n,l_1-1,l_2+1}).$$

In particular, $M_n \text{span}(\mathcal{V}_{n,l_1,l_2}) \subseteq \text{span}(\mathcal{V}_{n,l_1-1,l_2+1})$.

Proof. Let $z_{\omega_1,\omega_2,k,t} \in \mathcal{V}_{n,l_1,l_2}$ and $\mathbf{E} = \mathbf{G}_{\omega_1,\omega_2,k,t}$. Since $|\omega_1| \ge 2$, $\mathbf{E}$ contains strings with the same leading bit pair and the same trailing bit. Applying Theorem 2.3.2, we have

$$U_n z_{\omega_1,\omega_2,k,t} = U_n x_{\mathbf{E}} = u_j^{2i} x_{2\mathbf{E}} + u_j^{2i+1} x_{2\mathbf{E}+1} \qquad \text{for some } i, j.$$

From Theorem 2.6.1, $x_{2\mathbf{E}}$ and $x_{2\mathbf{E}+1}$ belong to $\mathcal{V}_{n,l_1-1,l_2+1}$. So $U_n x_{\mathbf{E}} \in \text{span}(\mathcal{V}_{n,l_1-1,l_2+1})$.
□

The dual action of M_n^* is an easy consequence of Theorem 2.6.2 once we determine how general indicial sets are affected by binary reversal. It is easily verified that for a general indicial set $\mathbf{G}_{\omega_1,\omega_2,k,t}$,

$$\begin{aligned}(\mathbf{G}_{\omega_1,\omega_2,k,t})^R &= \{\mu^R : \mu \in \mathbf{G}_{\omega_1,\omega_2,k,t}\} \\ &= \{\mu : \mu \in \mathbf{G}_{\omega_2^R,\omega_1^R,k,t}\} \\ &= \mathbf{G}_{\omega_2^R,\omega_1^R,k,t}.\end{aligned}$$

Thus $\tilde{R}_n z_{\omega_1,\omega_2,k,t} = z_{\omega_2^R,\omega_1^R,k,t}$ and $\tilde{R}_n \mathcal{V}_{n,l_1,l_2} = \mathcal{V}_{n,l_2,l_1}$.

Corollary 2.6.3 *Let $n \geq 3$, $l_2 \geq 2$ and $l_1 + l_2 \leq n$. Then*

$$M_n^* \text{span}(\mathcal{V}_{n,l_1,l_2}) \subseteq \text{span}(\mathcal{V}_{n,l_1+1,l_2-1}).$$

Proof. Recall that $\tilde{R}_n M_n^* \tilde{R}_n$ is duodiagonal (Theorem 2.4.1). Thus

$$\begin{aligned}\tilde{R}_n M_n^* \text{span}(\mathcal{V}_{n,l_1,l_2}) &= \tilde{R}_n M_n^* \tilde{R}_n \text{span}(\mathcal{V}_{n,l_2,l_1}) \\ &\subseteq \text{span}(\mathcal{V}_{n,l_2-1,l_1+1}) \quad \text{by Theorem 2.6.2,}\end{aligned}$$

and so

$$\begin{aligned}M_n^* \text{span}(\mathcal{V}_{n,l_1,l_2}) &\subseteq \tilde{R}_n \text{span}(\mathcal{V}_{n,l_2-1,l_1+1}) \\ &= \text{span}(\mathcal{V}_{n,l_1+1,l_2-1}).\end{aligned}$$

since $\tilde{R}_n^{-1} = \tilde{R}_n$. □

2.7 Choice of indicial bases and the spectral invariance conjecture

Recall that $\mathcal{S}_{n,l}$ is the set of all nonzero suffix-based indicial vectors $x^n_{\omega,k,t} \in \mathbf{R}^{2^n}$ with l-bit suffix ω, and that $\mathcal{T}_{n,l}$ is the corresponding prefix-based indicial basis. In Section 2.2, for fixed n and l, we chose $\text{span}(\mathcal{S}_{n,l})$ and $\text{span}(\mathcal{T}_{n,l})$ as the subspaces for approximating the top two column eigenvectors and the top two row eigenvectors of M_n. We now justify why these choices are best in a certain class of subspaces of the same dimension.

Recall from Section 2.6 that $\mathcal{S}_{n,l} = \mathcal{V}_{n,1,l}$ and $\mathcal{T}_{n,l} = \mathcal{V}_{n,l,1}$. We will show in Appendix A that the general indicial bases $\mathcal{V}_{n,1,l}$, $\mathcal{V}_{n,2,l-1}$, ..., $\mathcal{V}_{n,l,1}$ all have the same cardinality (see Corollary A.1.5) and so the subspaces $\text{span}(\mathcal{V}_{n,i,l+1-i})$, $i = 1, 2, \ldots, l$, all have

the same dimension. We claim that among these subspaces, $\mathrm{span}(\mathcal{V}_{n,1,l}) = \mathrm{span}(\mathcal{S}_{n,l})$ gives the best approximations to the top two column eigenvectors of M_n, and that $\mathrm{span}(\mathcal{V}_{n,l,1}) = \mathrm{span}(\mathcal{T}_{n,l})$ gives the best approximations to the top two row eigenvectors of M_n.

From the theory of the classical power method for computing dominant eigenvalues and eigenvectors, we know that for any real vector x and conformable matrix B, Bx has a "richer" component in the top column eigenvector than does x, and similarly for the second column eigenvector. So for $x \in \mathrm{span}(\mathcal{V}_{n,i,l+1-i})$, $i = 2,3,\ldots,l$, $M_n x$ has a richer component in the top column eigenvector q_1 of M_n than does x. But from Theorem 2.6.2, $M_n x \in \mathrm{span}(\mathcal{V}_{n,i-1,l+2-i})$. Therefore, the best approximation to q_1 from $\mathrm{span}(\mathcal{V}_{n,i-1,l+2-i})$ would be better than the best approximation to q_1 from $\mathrm{span}(\mathcal{V}_{n,i,l+1-i})$, $i = 2,3,\ldots,l$. In particular, the best approximation to q_1 from $\mathrm{span}(\mathcal{V}_{n,1,l}) = \mathrm{span}(\mathcal{S}_{n,l})$ would be better than any approximation to q_1 from $\mathrm{span}(\mathcal{V}_{n,i,l+1-i})$, $i = 2,3,\ldots,l$. So $\mathrm{span}(\mathcal{S}_{n,l})$ contains the best approximations to the top two column eigenvectors of M_n among $\mathrm{span}(\mathcal{V}_{n,i,l+1-i})$, $i = 1,2,\ldots,l$. A similar argument for M_n^* (and using Corollary 2.6.3) shows that $\mathrm{span}(\mathcal{T}_{n,l})$ contains the best approximations to the top two row eigenvectors of M_n among $\mathrm{span}(\mathcal{V}_{n,i,l+1-i})$, $i = 1,2,\ldots,l$.

What about the approximations to the top two eigenvalues of M_n? Would those two special subspaces give better approximations than the other general indicial subspaces? To answer these questions, let

$$P^C_{n,i,l+1-i} = D_X^{-1}(X^* M_n X), \qquad D_X = X^* X$$

where the columns of X are the vectors in $\mathcal{V}_{n,i,l+1-i}$, and let $P^R_{n,i,l+1-i} = D_X^{-1}(X^* M_n^* X)$. Then $P^C_{n,1,l} = P^C_{n,l}$ and $P^R_{n,l,1} = P^R_{n,l}$ as previously defined. We have the following remarkable

Theorem 2.7.1 (Spectral invariance) *The projection matrices* $P^C_{n,1,l}$, $P^C_{n,2,l-1}$, $\ldots$, $P^C_{n,l,1}$, $P^R_{n,1,l}$, $P^R_{n,2,l-1}$, $\ldots$, $P^R_{n,l,1}$ *all have the same set of eigenvalues.*

Chapter 3

Combinatorics of Indicial Subspaces

3.1 Quantitative analysis of 1-bit suffix-based indicial sets

In this section, we shall be solely concerned with the quantitative properties of suffix-based indicial sets of the form $\mathbf{I}^n_{\omega,k,t}$ with $|\omega| = 1$. As usual, n will be a fixed integer (and we omit it in writing indicial sets). We first determine the values of k (the 1-bit count) and t (the bit transition count) giving nonempty indicial sets, and the cardinalities of those sets. We then show that the largest indicial set has cardinality $\approx 2^n/n\pi$. Finally, we will prove that the number of nonempty indicial sets is $2 + n(\pi - 1) = O(n^2)$.

We now begin a formal analysis that will establish Theorem 3.1.2. There is a relation between k and t for strings ending in 0.

Lemma 3.1.1 *Consider nonempty indicial sets* $\mathbf{I}_{0,k,t}$. *Then*

(a) $t = 0$ *if* $k = 0$,

(b) $1 \leq t \leq \min(2k, 2(n-k)-1)$ *if* $1 \leq k \leq n-1$.

Proof. It is obvious that for $k = 0$, the only nonempty indicial set is $\mathbf{I}_{0,0,0} = \{\underbrace{0\ldots0}_{n}\}$.

Consider now a fixed $k \geq 1$. Since $k \geq 1$ and any string $\mu \in \mathbf{I}_{0,k,t}$ has trailing bit 0, there must be at least 1 bit transition within μ, i.e. $t \geq 1$. Suppose $\mu \in \mathbf{I}_{0,k,t}$ has at most as many 1's as 0's, i.e. $k \leq n-k$. Then each 1 in μ can contribute at most 2 bit transitions (if preceded and followed by 0's), and so $t \leq 2k$. If instead μ has at most as many 0's as

1's, i.e. $k \geq n-k$, then each 0 in μ contributes at most 2 bit transitions, except for the trailing 0, which contributes at most 1 bit transition. So $t \leq 2(n-k-1)+1 = 2(n-k)-1$. Combining the two cases yields $1 \leq t \leq \min(2k, 2(n-k)-1)$ for nonempty indicial sets $\mathbf{I}_{0,k,t}$, $k \geq 1$. □

The next task is to compute $|\mathbf{I}_{0,k,t}|$ for $1 \leq k \leq n-1, 1 \leq t \leq \min(2k, 2(n-k)-1)$. This will be accomplished by deriving an alternative characterization for $\mathbf{I}_{0,k,t}$.

Definition 3.1 *Let μ be a nonempty string. By a* block of 0's *in a string μ, we shall mean a (nonempty) sequence of 0's in μ which is preceded by (if possible) and followed by (if possible) by 1's. We make an analogous definition for a* block of 1's *in μ.*

> eg. $\mu = 1001110110$ has 3 blocks of 0's, 3 blocks of 1's, and $3+3-1 = 5$ bit transitions.

As the above example indicates, the bit transition count of a string μ is one less than the sum of its number of blocks of 0's and its number of blocks of 1's. We thus have the following alternative characterization for $\mathbf{I}_{0,k,t}$:

$$\mathbf{I}_{0,k,t} = \begin{cases} \{\mu \in \{0,1\}^m : \ \kappa(\mu) = k,\ \tau(\mu) = t,\ \mu(n) = 0, \text{ and } \mu \text{ has} \\ \qquad \tfrac{t}{2}+1 \text{ blocks of 0's and } \tfrac{t}{2} \text{ blocks of 1's}\} & \text{if } t \text{ even} \\ \{\mu \in \{0,1\}^m : \ \kappa(\mu) = k,\ \tau(\mu) = t,\ \mu(n) = 0, \text{ and } \mu \text{ has} \\ \qquad \tfrac{t+1}{2} \text{ blocks of 0's and } \tfrac{t+1}{2} \text{ blocks of 1's}\} & \text{if } t \text{ odd} \end{cases}$$

Theorem 3.1.2 *The cardinalities of the nonempty indicial sets $\mathbf{I}^n_{0,k,t}$ are given by:*

(a) $|\mathbf{I}^n_{0,0,0}| = 1$,

(b) for $1 \leq k \leq n-1$, $1 \leq t \leq \min(2k, 2(n-k)-1)$,

$$|\mathbf{I}^n_{0,k,t}| = \begin{cases} \binom{k-1}{t/2-1}\binom{n-k-1}{t/2} & \text{if } t \text{ even} \\ \binom{k-1}{(t-1)/2}\binom{n-k-1}{(t-1)/2} & \text{if } t \text{ odd} \end{cases}$$

Proof. Case (a) is trivially true. Let k and t be as in case (b). Consider $\mu \in \mathbf{I}_{0,k,t}$. Using the above characterization of $\mathbf{I}_{0,k,t}$, we see that if t is even, the k 1's and $n-k$ 0's of μ are divided into $t/2$ and $t/2+1$ blocks respectively; and that if t is odd, they are each divided into $(t+1)/2$ blocks. From combinatorics, we know that the number of ways to divide m 0's (or m 1's) into q nonempty blocks where the ordering of the blocks is important is given by $\begin{pmatrix} m-1 \\ q-1 \end{pmatrix}$. The result then follows by applying the combinatorial formula to the division of 0's and the division of 1's of μ into blocks. □

The cardinalites of the nonempty indicial sets $\mathbf{I}_{1,k,t}$ can be derived by a similar argument. We note, however, a particularly simple and useful relationship between these indicial sets and those of Theorem 3.1.2.

Definition 3.2 *Let μ be a nonempty string. The* ones complement $\overline{\mu}$ *of μ is the string obtained by reversing 0's and 1's. If E is a set of nonempty strings, we define* $\overline{\mathbf{E}} := \{\overline{\mu} : \mu \in \mathbf{E}\}$.

eg. $\overline{0110100} = 1001011$.

Proposition 3.1.3 *For all $n \geq 1$, $0 \leq k \leq n$ and $0 \leq t \leq n-1$,*

$$\overline{\mathbf{I}}_{0,k,t} = \mathbf{I}_{1,n-k,t} \quad \textit{and} \quad \overline{\mathbf{I}}_{1,k,t} = \mathbf{I}_{0,n-k,t}.$$

We thus have a one-to-one correspondence between the collection of nonempty $\mathbf{I}_{0,k,t}$ and the collection of nonempty $\mathbf{I}_{1,k,t}$ given by ones complementation, with corresponding indicial sets having the same cardinality. Making the transformation $k \rightarrow n-k$ in Theorem 3.1.2, we obtain the corresponding result for $|\mathbf{I}_{1,k,t}|$:

Corollary 3.1.4 *The cardinalities of the nonempty indicial sets $\mathbf{I}^n_{1,k,t}$ are given by:*

(a) $|\mathbf{I}^n_{1,n,0}| = 1$,

(b) for $1 \leq k \leq n-1$, $1 \leq t \leq \min(2k-1, 2(n-k))$,

$$|\mathbf{I}^n_{1,k,t}| = \begin{cases} \begin{pmatrix} k-1 \\ t/2 \end{pmatrix}\begin{pmatrix} n-k-1 \\ t/2-1 \end{pmatrix} & \textit{if } t \textit{ even} \\ \\ \begin{pmatrix} k-1 \\ (t-1)/2 \end{pmatrix}\begin{pmatrix} n-k-1 \\ (t-1)/2 \end{pmatrix} & \textit{if } t \textit{ odd} \end{cases}$$

Having determined the cardinalities of the nonempty indicial sets $\mathbf{I}_{\omega,k,t}$ with $|\omega| = 1$, we now turn to finding the maximum cardinality of such a set. Because of the one-to-one correspondence previously mentioned, we need only consider maximizing among the nonempty indicial sets $\mathbf{I}_{0,k,t}$.

We first recall the floor and ceiling functions for real numbers. For a real number α, $\lfloor\alpha\rfloor$ (floor of α) is the largest integer $\leq \alpha$, and $\lceil\alpha\rceil$ (ceiling of α) is the smallest integer $\geq \alpha$.

eg. $\lfloor 3.9\rfloor = \lceil 2.1\rceil = 3$ and $\lfloor -6.5\rfloor = \lceil -7.1\rceil = -7$.

We note that $\lfloor\alpha/2\rfloor + \lceil\alpha/2\rceil = \alpha$, $\lfloor -\alpha\rfloor = -\lceil\alpha\rceil$, $\lceil -\alpha\rceil = -\lfloor\alpha\rfloor$ for all real numbers α. In addition, for a positive integer m,

$$\max_{0\leq i\leq m} \binom{m}{i} = \binom{m}{\lfloor m/2\rfloor} = \binom{m}{\lceil m/2\rceil} \tag{3.1}$$

The following theorem gives the maximum cardinality of an indicial set $\mathbf{I}_{0,k,t}$. It then follows by Stirling's approximation that the maximum cardinality of a 1-bit suffix-based indicial set is $\approx 2^n/n\pi$. The proof of the theorem is tedious, and may be skipped without any loss of continuity.

Theorem 3.1.5 *Let $n \geq 1$. For $n \equiv 0, 1 \pmod 4$,*

$$\max_{k,t} |\mathbf{I}^n_{0,k,t}| = |\mathbf{I}^n_{0,\lfloor n/2\rfloor-1,2\lfloor n/4\rfloor}| = \binom{\lfloor n/2\rfloor - 2}{\lfloor n/4\rfloor - 1}\binom{\lceil n/2\rceil}{\lfloor n/4\rfloor},$$

and for $n \equiv 2, 3 \pmod 4$,

$$\max_{k,t} |\mathbf{I}^n_{0,k,t}| = |\mathbf{I}^n_{0,\lfloor n/2\rfloor,2\lfloor n/4\rfloor+1}| = \binom{\lfloor n/2\rfloor - 1}{\lfloor n/4\rfloor}\binom{\lceil n/2\rceil - 1}{\lfloor n/4\rfloor}.$$

Proof. We sketch the main ideas and leave the verification of the details to the reader.

Define

$$m_0 = \max_{\substack{k,t \\ t \text{ even}}} |\mathbf{I}_{0,k,t}| \quad \text{and} \quad m_1 = \max_{\substack{k,t \\ t \text{ odd}}} |\mathbf{I}_{0,k,t}|.$$

We seek $\max(m_0, m_1)$.

Consider first finding m_0. By Theorem 3.1.2,

$$m_0 = \max_{\substack{1 \le k \le n-1 \\ 1 \le t \le \min(2k, 2(n-k)-1),\ t \text{ even}}} \binom{k-1}{t/2-1}\binom{n-k-1}{t/2}$$

$$= \max_{\substack{1 \le k \le n-1 \\ 0 \le t' \le \min(k-1, n-k-2)}} f(k,t')$$

where $t' = t/2 - 1$ and $f(k,t') = \binom{k-1}{t'}\binom{n-k-1}{t'+1}$. For a fixed k,

$$f(k,t'+1) \ge f(k,t') \Leftrightarrow t'+1 \le \frac{k(n-k-1)}{n}.$$

So the value of t' maximizing $f(k,t')$ for fixed k is given by:

$$t' = \left\lfloor \frac{k(n-k-1)}{n} \right\rfloor \tag{3.2}$$

Similary, for a fixed t, we have $t'+1 \le k \le n-t'-2$ and

$$f(k+1,t') \ge f(k,t') \Leftrightarrow k+1 \le \frac{t'(n-1)}{1+2t'} + 1.$$

So the value of k maximizing $f(k,t')$ for fixed t' is given by:

$$k = \left\lfloor \frac{t'(n-1)}{1+2t'} \right\rfloor + 1 \tag{3.3}$$

By considering the possible values of n mod 4, we can show that

$$k = \lfloor n/2 \rfloor - 1, \quad t' = \lfloor n/4 \rfloor - 1$$

is a simultaneous solution to (3.2) and (3.3). Recalling the change of variables $t' = t/2 - 1$, we have

$$m_0 = |\mathbf{I}_{0,\lfloor n/2 \rfloor - 1, 2\lfloor n/4 \rfloor}| = \binom{\lfloor n/2 \rfloor - 2}{\lfloor n/4 \rfloor - 1}\binom{\lceil n/2 \rceil}{\lfloor n/4 \rfloor}.$$

Consider now finding m_1. By Theorem 3.1.2,

$$m_1 = \max_{\substack{1 \le k \le n-1 \\ 1 \le t \le \min(2k, 2(n-k)-1),\ t \text{ odd}}} \binom{k-1}{(t-1)/2}\binom{n-k-1}{(t-1)/2}$$

$$= \max_{\substack{1 \le k \le n-1 \\ 0 \le t' \le \min(k-1, n-k-1)}} g(k,t')$$

where $t' = (t-1)/2$ and $g(k,t') = \begin{pmatrix} k-1 \\ t' \end{pmatrix}\begin{pmatrix} n-k-1 \\ t' \end{pmatrix}$. Since $g(k,t') = g(n-k,t')$, we conclude by symmetry that for a fixed t', the value of k maximizing $g(k,t')$ is $k = \lfloor n/2 \rfloor$. So

$$m_1 = \max_{0 \le t' \le \lfloor n/2 \rfloor - 1} g(\lfloor n/2 \rfloor, t') = \max_{0 \le t' \le \lfloor n/2 \rfloor - 1} \begin{pmatrix} \lfloor n/2 \rfloor - 1 \\ t' \end{pmatrix}\begin{pmatrix} \lceil n/2 \rceil - 1 \\ t' \end{pmatrix}.$$

Since

$$\lfloor n/4 \rfloor = \left\lceil \frac{\lfloor n/2 \rfloor - 1}{2} \right\rceil \qquad \text{for all } n,$$

$$\text{and} \qquad \lfloor n/4 \rfloor = \begin{cases} \left\lceil \frac{\lceil n/2 \rceil - 1}{2} \right\rceil & \text{if } n \equiv 0,1,2 \pmod 4 \\ \\ \left\lfloor \frac{\lceil n/2 \rceil - 1}{2} \right\rfloor & \text{if } n \equiv 3 \pmod 4 \end{cases}$$

we conclude by formula (3.1) that $t' = \lfloor n/4 \rfloor$ gives the maximum value. Recalling the change of variables $t' = (t-1)/2$, we have

$$m_1 = |\mathbf{I}_{0,\lfloor n/2 \rfloor, 2\lfloor n/4 \rfloor + 1}| = \begin{pmatrix} \lfloor n/2 \rfloor - 1 \\ \lfloor n/4 \rfloor \end{pmatrix}\begin{pmatrix} \lceil n/2 \rceil - 1 \\ \lfloor n/4 \rfloor \end{pmatrix}.$$

We now find $\max(m_0, m_1)$. It is easily verified that

$$\frac{m_1}{m_0} = \frac{(\lfloor n/2 \rfloor - 1)(\lceil n/2 \rceil - \lfloor n/4 \rfloor)}{\lfloor n/4 \rfloor \lceil n/2 \rceil},$$

and that

$$\begin{aligned} m_1 > m_0 \quad &\Leftrightarrow \quad \lceil n/2 \rceil (\lfloor n/2 \rfloor - 1) > \lfloor n/4 \rfloor (n-1) \\ &\Leftrightarrow \quad n \equiv 2,3 \pmod 4. \end{aligned}$$

The theorem then follows. □

Recalling that $\bar{\mathbf{I}}_{0,k,t} = \mathbf{I}_{1,n-k,t}$, we obtain the corresponding result for nonempty $\mathbf{I}_{1,k,t}$ by making the transformation $k \to n-k$:

Corollary 3.1.6 *Let $n \ge 1$. For $n \equiv 0,1 \pmod 4$,*

$$\max_{k,t} |\mathbf{I}^n_{1,k,t}| = |\mathbf{I}^n_{1,\lceil n/2 \rceil + 1, 2\lfloor n/4 \rfloor}| = \begin{pmatrix} \lceil n/2 \rceil \\ \lfloor n/4 \rfloor \end{pmatrix}\begin{pmatrix} \lfloor n/2 \rfloor - 2 \\ \lfloor n/4 \rfloor - 1 \end{pmatrix},$$

and for $n \equiv 2,3 \pmod 4$,

$$\max_{k,t} |\mathbf{I}^n_{1,k,t}| = |\mathbf{I}^n_{1,\lceil n/2\rceil, 2\lfloor n/4\rfloor+1}| = \left(\begin{array}{c} \lceil n/2\rceil - 1 \\ \lfloor n/4\rfloor \end{array} \right) \left(\begin{array}{c} \lfloor n/2\rfloor - 1 \\ \lfloor n/4\rfloor \end{array} \right).$$

We now count the number of nonempty indicial sets $\mathbf{I}_{\omega,k,t}$ with $|\omega| = 1$. This is easily accomplished using the bounds on k and t from Theorem 3.1.2.

Theorem 3.1.7 *The number of nonempty indicial sets* $\mathbf{I}_{\omega,k,t}$ *with* $|\omega| = 1$ *is* $2 + n(n-1)$.

Proof. By Theorem 3.1.2, the number of nonempty $\mathbf{I}_{0,k,t}$ is:

$$\begin{aligned} 1 + \sum_{k=1}^{n-1} \min(2k, 2(n-k)-1) &= 1 + \sum_{k=1}^{n-1} k \quad \text{(after some simplification)} \\ &= 1 + \frac{n(n-1)}{2}. \end{aligned}$$

From the one-to-one correspondence between nonempty $\mathbf{I}_{0,k,t}$ and nonempty $\mathbf{I}_{1,k,t}$, we deduce that the number of nonempty $\mathbf{I}_{1,k,t}$ is also $1 + n(n-1)/2$, and we have the desired count. □

3.2 Reduction principle for indicial sets

Our goal in this section is to prove a reduction principle relating arbitrary suffix-based indicial sets to 1-bit suffix-based indicial sets. We can then apply the principle to extend the results of Section 3.1.

The reduction principle transforms indicial sets $\mathbf{I}^n_{\omega,k,t}$ with $|\omega| = l$ to 1-bit indicial sets by dropping the last $l-1$ bits of strings in $\mathbf{I}^n_{\omega,k,t}$. Central to the proof of the principle are the following fundamental equalities for the 1-bit count and bit transition count of a nonempty string.

Proposition 3.2.1 *Let* $n \geq 1$ *and* $\mu \in \{0,1\}^n$. *Then*

$$\begin{aligned} \kappa(\mu) &= \kappa(\mu(1) \circ \cdots \circ \mu(n-l+1)) + \kappa(\mu(n-l+2) \circ \cdots \circ \mu(n)) \\ \text{and} \quad \tau(\mu) &= \tau(\mu(1) \circ \cdots \circ \mu(n-l+1)) + \tau(\mu(n-l+1) \circ \cdots \circ \mu(n)). \end{aligned}$$

We first show that dropping the last $l-1$ bits of strings in $\mathbf{I}^n_{\omega,k,t}$ does indeed transform it into a 1-bit indicial set.

Lemma 3.2.2 *Let n and l be positive integers, with $n \geq 2$ and $2 \leq l \leq n$, and let ω be a string of length l. Then*

$$\{\mu(1) \circ \cdots \circ \mu(n-l+1) : \mu \in \mathbf{I}^n_{\omega,k,t}\} \quad = \quad \mathbf{I}^{n-l+1}_{\omega(1),k-k',t'}$$

where

$$\begin{aligned} k' &= \kappa(\omega(2) \circ \cdots \circ \omega(l)) \\ \textit{and} \qquad t' &= t - \tau(\omega). \end{aligned}$$

Proof. Let $\mu \in \mathbf{I}^n_{\omega,k,t}$ and $\mu' = \mu(1) \circ \cdots \circ \mu(n-l+1)$. Then

$$\begin{aligned} \mu(n-l+1) \circ \cdots \circ \mu(n) &= \omega, \\ \kappa(\mu') &= \kappa(\mu) - \kappa(\mu(n-l+2) \circ \cdots \circ \mu(n)) \quad \text{by Proposition 3.2.1} \\ &= k - k', \\ \text{and} \quad \tau(\mu') &= \tau(\mu) - \tau(\mu(n-l+1) \circ \cdots \circ \mu(n)) \quad \text{by Proposition 3.2.1} \\ &= t'. \end{aligned}$$

So $\mu' \in \mathbf{I}^{n-l+1}_{\omega(1),k-k',t'}$.

Conversely, let $\mu' \in \mathbf{I}^{n-l+1}_{\omega(1),k-k',t'}$, and $\mu = \mu' \circ [\omega(2) \circ \cdots \circ \omega(l)] = \mu'(1) \circ \cdots \circ \mu'(n-l) \circ \omega(1) \circ [\omega(2) \circ \cdots \circ \omega(l)]$. Then

$$\begin{aligned} \mu(n-l+1) \circ \cdots \circ \mu(n) &= \omega, \\ \kappa(\mu) &= \kappa(\mu') + \kappa(\omega(2) \circ \cdots \circ \omega(l)) \quad \text{by Proposition 3.2.1} \\ &= k, \\ \text{and} \quad \tau(\mu) &= \tau(\mu') + \tau(\omega(1) \circ \omega(2) \circ \cdots \circ \omega(l)) \quad \text{by Proposition 3.2.1} \\ &= t. \end{aligned}$$

So $\mu \in \mathbf{I}^n_{\omega,k,t}$ and $\mu' = \mu(1) \circ \cdots \circ \mu(n-l+1)$. □

Theorem 3.2.3 *Let n and l be positive integers, with $n \geq 2$ and $2 \leq l \leq n$, and let ω be a fixed string of length l. There exists a one-to-one correspondence between the collection $\mathcal{I}^n_l$ of nonempty suffix-based indicial sets $\mathbf{I}^n_{\omega,k,t}$ and the collection $\mathcal{I}^{n-l+1}_1$ of nonempty 1-bit suffix-based indicial sets $\mathbf{I}^{n-l+1}_{\omega(1),k,t}$. Furthermore, corresponding indicial sets have the same cardinality.*

Proof. Define the function $f : \mathcal{I}_l^n \to \mathcal{I}_1^{n-l+1}$ by:

$$f(\mathbf{I}^n_{\omega,k,t}) = \{\mu(1) \circ \cdots \circ \mu(n-l+1) : \mu \in \mathbf{I}^n_{\omega,k,t}\}.$$

From Lemma 3.2.2, $f(\mathbf{I}^n_{\omega,k,t}) = \mathbf{I}^{n-l+1}_{\omega(1),k-k',t'}$ where

$$k' = \kappa(\omega(2) \circ \cdots \circ \omega(l))$$

$$\text{and} \qquad t' = t - \tau(\omega).$$

We show that f is a one-to-one correspondence between $\mathcal{I}_l^n$ and $\mathcal{I}_1^{n-l+1}$ with the desired property.

Suppose $f(\mathbf{I}^n_{\omega,k_1,t_1}) = f(\mathbf{I}^n_{\omega,k_2,t_2})$ for some $\mathbf{I}^n_{\omega,k_1,t_1}, \mathbf{I}^n_{\omega,k_2,t_2} \in \mathcal{I}_l^n$. Then

$$\mathbf{I}^{n-l+1}_{\omega(1),k_1-k',t_1-\tau(\omega)} = \mathbf{I}^{n-l+1}_{\omega(1),k_2-k',t_2-\tau(\omega)}$$

and so $k_1 = k_2$ and $t_1 = t_2$. Thus f is one-to-one. Furthermore, f is onto $\mathcal{I}_1^{n-l+1}$ since for $\mathbf{I}^{n-l+1}_{\omega(1),k,t} \in \mathcal{I}_1^{n-l+1}$, $\mathbf{I}^n_{\omega,k+k',t+\tau(\omega)} \in \mathcal{I}_l^n$ and $f(\mathbf{I}^n_{\omega,k+k',t+\tau(\omega)}) = \mathbf{I}^{n-l+1}_{\omega(1),k,t}$. Finally, for $\mathbf{I}^n_{\omega,k,t} \in \mathcal{I}_l^n$, $f(\mathbf{I}^n_{\omega,k,t})$ and $\mathbf{I}^n_{\omega,k,t}$ have the same cardinality since for $\mu_1, \mu_2 \in \mathbf{I}^n_{\omega,k,t}$,

$$\mu_1 \neq \mu_2 \quad \Rightarrow \quad \mu_1(1) \circ \cdots \circ \mu_1(n-l) \neq \mu_2(1) \circ \cdots \circ \mu_2(n-l)$$

because

$$\mu_1(n-l+1) \circ \cdots \circ \mu_1(n) = \mu_2(n-l+1) \circ \cdots \circ \mu_2(n) = \omega. \quad \square$$

There is a similar reduction principle relating general indicial sets to suffix-based indicial sets. We refer the interested reader to Appendix A for its statement and proof.

3.3 Quantitative properties of suffix-based indicial sets and projection matrices

In this section, we extend the results of Section 3.1 to arbitrary suffix-based indicial sets using the reduction principle proved in Section 3.2. We can then deduce the order of our projection matrices (or equivalently, the cardinalities of our indicial bases) and the number of nonzero entries in them. We shall in fact show that the indicial bases $\mathcal{S}_{n,l}$ and $\mathcal{T}_{n,l}$ both have cardinality

$$2^l(1 + \frac{(n-l+1)(n-l)}{2}) < n^2 2^{l-1}.$$

Before we begin a formal analysis, we present some numerical results to get a feel for the quantitative behaviour of our indicial subspaces. Table 3.1 gives the cardinality of the indicial basis $\mathcal{S}_{n,l}$ and the maximum size of an indicial set $\mathbf{I}^n_{\omega,k,t}$ (with $|\omega| = l$) for $l = 2, 4$. The latter quantity is by definition equal to the maximum number of ones appearing in a basis vector in $\mathcal{S}_{n,l}$. We see from the table that the indicial bases have cardinalities which are very small compared to 2^n; in contrast, the basis vectors have a large number of nonzero entries. For example, for $n = 30$ and $l = 2$, we approximate $\mathbf{R}^{2^{30}}$ by the subspace spanned by the 1628 basis vectors in $\mathcal{S}_{30,2}$, the "largest" of which has 5.95×10^6 ones appearing in it.

n	2^n	$\lvert\mathcal{S}_{n,2}\rvert$	$\max_{\substack{\omega,k,t \\ \lvert\omega\rvert = 2}} \lvert\mathbf{I}^n_{\omega,k,t}\rvert$	$\lvert\mathcal{S}_{n,4}\rvert$	$\max_{\substack{\omega,k,t \\ \lvert\omega\rvert = 4}} \lvert\mathbf{I}^n_{\omega,k,t}\rvert$
5	32	28	2	32	1
10	1024	148	20	352	6
15	32768	368	400	1072	120
20	1.05×10^6	688	8820	2192	2520
25	3.36×10^7	1108	2.33×10^5	3712	63504
30	1.07×10^9	1628	5.95×10^6	5632	1.59×10^6

Table 3.1: *Combinatorial properties of suffix-based indicial sets*

We now turn to extending the results of Section 3.1. Let n and l be fixed positive integers with $l \leq n$. From Theorem 3.2.3, there is a one-to-one correspondence f between the collection of nonempty suffix-based indicial sets $\mathbf{I}^n_{\omega,k,t}$ (for a fixed $\omega \in \{0,1\}^l$) and the collection of nonempty 1-bit suffix-based indicial sets $\mathbf{I}^{n-l+1}_{\omega(1),k,t}$ given by:

$$f(\mathbf{I}^n_{\omega,k,t}) = \mathbf{I}^{n-l+1}_{\omega(1),k-\kappa(\omega(2)\circ\cdots\circ\omega(l)),t-\tau(\omega)}.$$

By making the appropriate substitutions (n by $n-l+1$, k by $k-\kappa(\omega(2)\circ\cdots\circ\omega(l))$ and t by $t-\tau(\omega)$) in Theorems 3.1.2 and 3.1.5 and Corollaries 3.1.4 and 3.1.6 of Section 3.1, we obtain corresponding results for nonempty $\mathbf{I}^n_{\omega,k,t}$.

Theorem 3.3.1 *Let n be a positive integer, and ω be a fixed string of length $l \leq n$. Let $k' = \kappa(\omega(2)\circ\cdots\circ\omega(l))$. The cardinalities of the nonempty indicial sets $\mathbf{I}^n_{\omega,k,t}$ are given by:*

(a) if $\omega(1) = 0$:

(i) $|\mathbf{I}^n_{\omega,k',\tau(\omega)}| = 1$,

(ii) for $k'+1 \le k \le n-l+k'$, $\tau(\omega)+1 \le t \le \tau(\omega)+\min(2(k-k'),2(n-l-k+k')+1)$,

$$|\mathbf{I}^n_{\omega,k,t}| = \begin{cases} \left(\begin{array}{c} k-k'-1 \\ (t-\tau(\omega))/2-1 \end{array}\right)\left(\begin{array}{c} n-l-k+k' \\ (t-\tau(\omega))/2 \end{array}\right) & \text{if } t \equiv \tau(\omega) \pmod 2 \\ \left(\begin{array}{c} k-k'-1 \\ (t-\tau(\omega)-1)/2 \end{array}\right)\left(\begin{array}{c} n-l-k+k' \\ (t-\tau(\omega)-1)/2 \end{array}\right) & \text{if } t \equiv \tau(\omega)+1 \pmod 2 \end{cases}$$

(b) if $\omega(1) = 1$*:*

(i) $|\mathbf{I}^n_{\omega,n-l+k'+1,\tau(\omega)}| = 1$,

(ii) for $k'+1 \le k \le n-l+k'$, $\tau(\omega)+1 \le t \le \tau(\omega)+\min(2(k-k')-1,2(n-l-k+k'+1))$,

$$|\mathbf{I}^n_{\omega,k,t}| = \begin{cases} \left(\begin{array}{c} k-k'-1 \\ (t-\tau(\omega))/2 \end{array}\right)\left(\begin{array}{c} n-l-k+k' \\ (t-\tau(\omega))/2-1 \end{array}\right) & \text{if } t \equiv \tau(\omega) \pmod 2 \\ \left(\begin{array}{c} k-k'-1 \\ (t-\tau(\omega)-1)/2 \end{array}\right)\left(\begin{array}{c} n-l-k+k' \\ (t-\tau(\omega)-1)/2 \end{array}\right) & \text{if } t \equiv \tau(\omega)+1 \pmod 2 \end{cases}$$

Theorem 3.3.2 *Let* n *be a positive integer* ≥ 1, *and* ω *be a fixed string of length* $l \le n$. *Let* $k' = \kappa(\omega(2) \circ \cdots \circ \omega(l))$. *For* $n \equiv l-1, l \pmod 4$,

$$\begin{aligned} \max_{k,t} |\mathbf{I}^n_{\omega,k,t}| &= \left(\begin{array}{c} \lfloor (n-l+1)/2 \rfloor - 2 \\ \lfloor (n-l+1)/4 \rfloor - 1 \end{array}\right)\left(\begin{array}{c} \lceil (n-l+1)/2 \rceil \\ \lfloor (n-l+1)/4 \rfloor \end{array}\right) \\ &= \begin{cases} |\mathbf{I}^n_{\omega,\lfloor (n-l+1)/2 \rfloor + k' - 1, 2\lfloor (n-l+1)/4 \rfloor + \tau(\omega)}| & \text{if } \omega(1) = 0 \\ |\mathbf{I}^n_{\omega,\lceil (n-l+1)/2 \rceil + k' + 1, 2\lfloor (n-l+1)/4 \rfloor + \tau(\omega)}| & \text{if } \omega(1) = 1 \end{cases} \end{aligned}$$

and for $n \equiv l+1, l+2 \pmod 4$,

$$\begin{aligned} \max_{k,t} |\mathbf{I}^n_{\omega,k,t}| &= \left(\begin{array}{c} \lfloor (n-l+1)/2 \rfloor - 1 \\ \lfloor (n-l+1)/4 \rfloor \end{array}\right)\left(\begin{array}{c} \lceil (n-l+1)/2 \rceil - 1 \\ \lfloor (n-l+1)/4 \rfloor \end{array}\right) \\ &= \begin{cases} |\mathbf{I}^n_{\omega,\lfloor (n-l+1)/2 \rfloor + k', 2\lfloor (n-l+1)/4 \rfloor + \tau(\omega)+1}| & \text{if } \omega(1) = 0 \\ |\mathbf{I}^n_{\omega,\lceil (n-l+1)/2 \rceil + k', 2\lfloor (n-l+1)/4 \rfloor + \tau(\omega)+1}| & \text{if } \omega(1) = 1 \end{cases} \end{aligned}$$

Our next task is to count the number of nonempty suffix-based indicial sets $\mathbf{I}^n_{\omega,k,t}$ with $|\omega| = l$.

Theorem 3.3.3 *The number of nonempty indicial sets* $\mathbf{I}^n_{\omega,k,t}$ *with* $|\omega| = l > 0$ *is*

$$2^l\,(1 + \frac{(n-l+1)(n-l)}{2}) < n^2 2^{l-1}.$$

Proof. Let ω be a fixed string of length l. From the proof of Theorem 3.1.7, we know that there are $1+(n-l+1)(n-l)/2$ nonempty indicial sets of the form $\mathbf{I}^{n-l+1}_{\omega(1),k,t}$; by Theorem 3.2.3, we have exactly that many nonempty indicial sets of the form $\mathbf{I}^n_{\omega,k,t}$. Summing over the 2^l possible ω's, we obtain the desired count. □

We apply the above results to finding the order and the number of nonzero entries of the column projection matrix $P^C_{n,l}$ and of the row projection matrix $P^R_{n,l}$ for $l > 0$. We note that these two matrices have the same order and the same number of nonzero entries (see Section 2.4).

An immediate corollary to Theorem 3.3.3 gives us the order of the projection matrices:

Corollary 3.3.4 *The cardinality of the indicial bases* $S_{n,l}$ *and* $T_{n,l}$, $l > 0$, *are both* $2^l\,(1 + (n-l+1)(n-l)/2)$. *Consequently, the projection matrices* $P^C_{n,l}$ *and* $P^R_{n,l}$, $l > 0$, *both have order* $2^l\,(1 + (n-l+1)(n-l)/2)$.

Our final result concerns the number of nonzero entries in the projection matrices.

Theorem 3.3.5 *The number of nonzero entries in each of* $P^C_{n,l}$ *and* $P^R_{n,l}$, $l > 0$, *is*

$$2^{l+2}\,(1 + \frac{(n-l)(n-l-1)}{2}).$$

Proof. Referring to the analysis of the possible nonzero inner products occuring in the construction of the column projection matrix $P^C_{n,l}$ (see Section 2.4), we see that the number of nonzero entries in $P^C_{n,l}$ is $2\,(|\mathcal{E}^0| + |\mathcal{E}^1|)$, where

$$\mathcal{E}^0 = \{\text{nonempty } \mathbf{E}^0 \text{ where } \mathbf{E} = \mathbf{I}_{\omega,k,t} \text{ with } |\omega| = l\}$$

$$\text{and} \quad \mathcal{E}^1 = \{\text{nonempty } \mathbf{E}^1 \text{ where } \mathbf{E} = \mathbf{I}_{\omega,k,t} \text{ with } |\omega| = l\}.$$

We remind the reader that $\mathbf{E}^0$ and $\mathbf{E}^1$ are subsets of strings in $\mathbf{E}$ having 2^{nd} leading bit 0 and 1 respectively.

Again using the fact (Proposition 2.1.3) that the trailing bit and transition count t of a string determines its leading bit, we see that each $\mathbf{E}^0 \in \mathcal{E}^0$ is equal to some $\mathbf{G}_{\omega_1 o 0,\omega,k,t}$

with $|\omega_1| = 1$ and $|\omega| = l$, and that each nonempty $\mathbf{G}_{\omega_1 o 0,\omega,k,t}$ with $|\omega_1| = 1$ and $|\omega| = l$ is in $\mathcal{E}^0$. Thus $\mathcal{E}^0 = \{\text{nonempty } \mathbf{G}_{\omega_1 o 0,\omega,k,t} \text{ with } |\omega_1| = 1 \text{ and } |\omega| = l\}$. Similarly, $\mathcal{E}^1 = \{\text{nonempty } \mathbf{G}_{\omega_1 o 1,\omega,k,t} \text{ with } |\omega_1| = 1 \text{ and } |\omega| = l\}$. Therefore

$$\mathcal{E}^0 \cup \mathcal{E}^1 = \{\text{nonempty } \mathbf{G}_{\omega_1,\omega,k,t} \text{ with } |\omega_1| = 2 \text{ and } |\omega| = l\}.$$

Since $\mathcal{E}^0 \cap \mathcal{E}^1 = \emptyset$, we have

$$\begin{aligned} 2(|\mathcal{E}^0| + |\mathcal{E}^1|) &= 2 \cdot |\mathcal{E}^0 \cup \mathcal{E}^1| \\ &= 2 \cdot |\{\text{nonempty } \mathbf{I}_{\omega,k,t} \text{ with } \omega = l+1\}| \quad \text{by Theorem A.1.4} \\ &= 2^{l+2}(1 + \frac{(n-l)(n-l-1)}{2}) \quad \text{by Theorem 3.3.3. } \square \end{aligned}$$

Appendix A

Reduction principle for general indicial sets

In Section 3.2, we proved a reduction principle (Theorem 3.2.3) relating suffix-based indicial sets to 1-bit suffix-based indicial sets. Our goal in this appendix is to prove a similar reduction principle relating general indicial sets (defined in Section 2.6) to suffix-based indicial sets.

We first introduce the shift operators $+$ and $-$ on bit strings. For a nonempty string $\omega = \omega(1) \circ \omega(2) \circ \cdots \circ \omega(|\omega|)$, we define

$$\begin{aligned} \omega + 1 &:= \omega(2) \circ \omega(3) \circ \cdots \circ \omega(|\omega|) \circ \omega(1), \\ \omega - 1 &:= \omega(|\omega|) \circ \omega(1) \circ \cdots \circ \omega(|\omega|-1). \end{aligned}$$

We also define $\varepsilon + 1 = \varepsilon - 1 = \varepsilon$. The result of applying $+$ i times on a nonempty ω $(1 \leq i < |\omega|)$ will be denoted by $\omega + i$, and that of applying $-$ i times by $\omega - i$. Thus

$$\begin{aligned} \omega + i &:= \omega(i+1) \circ \omega(i+2) \circ \cdots \circ \omega(|\omega|) \circ \omega(1) \circ \cdots \circ \omega(i), \\ \omega - i &:= \omega(|\omega|-i+1) \circ \omega(|\omega|-i+2) \circ \cdots \circ \omega(|\omega|) \circ \omega(1) \circ \cdots \circ \omega(|\omega|-i). \end{aligned}$$

Note that

$$(\omega \pm i)(k) = \omega((k \pm i - 1) \bmod |\omega| + 1), \qquad k = 1, \ldots, |\omega|. \tag{A.1}$$

If $\mathbf{E} \subseteq \{0,1\}^m$ is a set of strings of length m, $m \geq 2$, we define $\mathbf{E} + i := \{\omega + i : \omega \in \mathbf{E}\}$ and $\mathbf{E} - i := \{\omega - i : \omega \in \mathbf{E}\}$ for $1 \leq i < m$.

We note the following properties of the operators $+$ and $-$.

Proposition A.1.1 *Let m be an integer ≥ 2, and let $\omega_1, \omega_2 \in \{0,1\}^m$, and $\mathbf{E}_1, \mathbf{E}_2 \subseteq \{0,1\}^m$. Then for $1 \leq i < m$, the following equivalences hold:*

$$\omega_1 = \omega_2 \Leftrightarrow \omega_1 \pm i = \omega_2 \pm i,$$
$$\textit{and} \quad \mathbf{E}_1 = \mathbf{E}_2 \Leftrightarrow \mathbf{E}_1 \pm i = \mathbf{E}_2 \pm i.$$

Proposition A.1.2 *Let m be an integer ≥ 2, and let $\omega \in \{0,1\}^m$, and $\mathbf{E} \subseteq \{0,1\}^m$. Then for $1 \leq i < m$,*

$$(\omega + i) - i = (\omega - i) + i = \omega,$$
$$\textit{and} \quad (\mathbf{E} + i) - i = (\mathbf{E} - i) + i = \mathbf{E}.$$

We also have the following relationships between the 1-bit count and the transition count of ω, $\omega + i$ and $\omega - i$:

$$\kappa(\omega \pm i) = \kappa(\omega), \tag{A.2}$$
$$\tau(\omega + i) = \tau(\omega) - \tau(\omega(i) \circ \omega(i+1)) + \tau(\omega(|\omega|) \circ \omega(1)), \tag{A.3}$$
$$\text{and} \quad \tau(\omega - i) = \tau(\omega) - \tau(\omega(|\omega|-i) \circ \omega(|\omega|-i+1)) + \tau(\omega(|\omega|) \circ \omega(1)). \tag{A.4}$$

Formulae (A.3) and (A.4) arise from the fundamental equality for the transition count of a nonempty string μ (cf. Proposition 3.2.1):

$$\tau(\mu) = \tau(\mu(1) \circ \mu(2)) + \tau(\mu(2) \circ \mu(3)) + \cdots + \tau(\mu(|\mu|-1) \circ \mu(|\mu|)).$$

As usual, we let n be a fixed integer ≥ 3. By performing appropriate shifts, we can transform general indicial sets to suffix-based ones, and vice versa. This forms the basis of Theorem A.1.4 below.

Lemma A.1.3 *Let l_1 and l_2 be positive integers, with $2 \leq l_1 + l_2 \leq n$. Let $\mathbf{G}_{\omega_1,\omega_2,k,t}$ be a nonempty general indicial set with $|\omega_1| = l_1$ and $|\omega_2| = l_2$. Then*

$$(\mathbf{G}_{\omega_1,\omega_2,k,t}) + (l_1 - 1) = \mathbf{G}_{\omega_1(l_1),\omega',k,t'} = \mathbf{I}_{\omega',k,t'},$$

where

$$\omega' = \omega_2 \circ \omega_1(1) \circ \cdots \circ \omega_1(l_1-1), \tag{A.5}$$
$$\text{and} \quad t' = t - \tau(\omega_1(l_1-1) \circ \omega_1(l_1)) + \tau(\omega_2(l_2) \circ \omega_1(1)). \tag{A.6}$$

Proof. The equality

$$\mathbf{G}_{\omega_1(l_1),\omega',k,t'} = \mathbf{I}_{\omega',k,t'}$$

follows from the fact that the trailing bit and the parity of the transition count of a nonempty string determines its leading bit (Proposition 2.1.3).

Let $\mu \in \mathbf{G}_{\omega_1,\omega_2,k,t}$ and $\mu' = \mu + (l_1 - 1)$. By definition, $\mu(1) \circ \cdots \circ \mu(l_1) = \omega_1$, and $\mu(n-l_2+1) \circ \cdots \circ \mu(n) = \omega_2$. Then

$$\begin{aligned}
\kappa(\mu') &= k \quad \text{by formula (A.2)},\\
\tau(\mu') &= \tau(\mu) - \tau(\mu(l_1-1) \circ \mu(l_1)) + \tau(\mu(n) \circ \mu(1)) \quad \text{by formula (A.3)}\\
&= t - \tau(\omega_1(l_1-1) \circ \omega_1(l_1)) + \tau(\omega_2(l_2) \circ \omega_1(1))\\
&= t' \quad \text{by formula (A.6)},\\
\mu'(n-l+2) \circ \cdots \circ \mu'(n) &= [\mu'(n-l_1-l_2+2) \circ \cdots \circ \mu'(n-l_1+1)] \circ\\
&\qquad [\mu'(n-l_1+2) \circ \cdots \circ \mu'(n)]\\
&= [\mu(n-l_2+1) \circ \cdots \circ \mu(n)] \circ [\mu(1) \circ \cdots \circ \mu(l_1-1)]\\
&= \omega_2 \circ \omega_1(1) \circ \omega_1(2) \circ \cdots \circ \omega_1(l_1-1),\\
&= \omega' \quad \text{by formula (A.5)},\\
\text{and } \mu'(1) &= (\mu + (l_1 - 1))(1)\\
&= \mu((l_1 - 1) \bmod n + 1) \quad \text{by formula (A.1)}\\
&= \mu(l_1)\\
&\quad \omega_1(l_1).
\end{aligned}$$

So $\mu' \in \mathbf{G}_{\omega_1(l_1),\omega',k,t'}$ and $(\mathbf{G}_{\omega_1,\omega_2,k,t}) + (l_1 - 1) \subseteq \mathbf{G}_{\omega_1(l_1),\omega',k,t'}$.

Conversely, let $\mu' \in \mathbf{G}_{\omega_1(l_1),\omega',k,t'}$, and $\mu = \mu' - (l_1 - 1)$. By definition, $\mu'(1) = \omega_1(l_1)$ and $\mu'(n-l_1-l_2+2) \circ \cdots \circ \mu'(n) = \omega_2 \circ \omega_1(1) \circ \cdots \circ \omega_1(l_1-1)$. Then

$$\begin{aligned}
\kappa(\mu) &= k \quad \text{by formula (A.2)},\\
\tau(\mu) &= t' - \tau(\mu'(n-l_1+1) \circ \mu'(n-l_1+2)) + \tau(\mu'(n) \circ \mu'(1))\\
&\qquad \text{by formula (A.4)}\\
&= t' - \tau(\omega_2(l_2) \circ \omega_1(1)) + \tau(\omega_1(l_1-1) \circ \omega_1(l_1))\\
&= t \quad \text{by formula (A.6)},\\
\mu(1) \circ \cdots \circ \mu(l_1) &= [\mu'(n-l_1+2) \circ \cdots \circ \mu'(n)] \circ \mu'(1)
\end{aligned}$$

$$
\begin{aligned}
& = [\omega_1(1) \circ \cdots \circ \omega_1(l_1-1)] \circ \omega_1(l_1) \\
& = \omega_1, \\
\text{and } \mu(n-l_2+1) \circ \cdots \circ \mu(n) & = \mu'(n-l_1-l_2+2) \circ \cdots \circ \mu'(n-l_1+1) \\
& = \omega_2.
\end{aligned}
$$

So $\mu \in \mathbf{G}_{\omega_1,\omega_2,k,t}$ and $\mu' = [\mu' - (l_1 - 1)] + (l_1 - 1) = \mu + (l_1 - 1)$. Thus $\mathbf{G}_{\omega_1(l_1),\omega',k,t'} \subseteq (\mathbf{G}_{\omega_1,\omega_2,k,t}) + (l_1 - 1)$. □

Theorem A.1.4 *Let l, l_1 and l_2 be positive integers, with $2 \leq l \leq n$ and $l_1 + l_2 = l$. There exists a one-to-one correspondence between the collection $\mathcal{G}_{l_1,l_2}$ of nonempty general indicial sets $\mathbf{G}_{\omega_1,\omega_2,k,t}$ with $|\omega_1| = l_1$ and $|\omega_2| = l_2$, and the collection $\mathcal{I}_{l-1}$ of nonempty suffix-based indicial sets $\mathbf{I}_{\omega,k,t}$ with $|\omega| = l - 1$. Furthermore, corresponding nonempty indicial sets have the same cardinality.*

Proof. We first consider the case $l_1 = 1$. Recall that the trailing bit and the transition count of a bit string determines its leading bit (Proposition 2.1.3). So for $\mathbf{G}_{\omega_1,\omega_2,k,t} \in \mathcal{G}_{1,l_2}$, we have $\mathbf{G}_{\omega_1,\omega_2,k,t} = \mathbf{I}_{\omega_2,k,t}$; and for $\mathbf{I}_{\omega,k,t} \in \mathcal{I}_{l_2}$, we have $\mathbf{I}_{\omega,k,t} = \mathbf{G}_{\omega',\omega,k,t}$ for some 1-bit string ω'. Thus $\mathcal{G}_{1,l_2} = \mathcal{I}_{l_2}$, and we have a trivial one-to-one correspondence.

Consider now the case $l_1 > 1$. From Lemma A.1.3, we know that for $\mathbf{G}_{\omega_1,\omega_2,k,t} \in \mathcal{G}_{l_1,l_2}$,

$$(\mathbf{G}_{\omega_1,\omega_2,k,t}) + (l_1 - 1) \in \mathcal{I}_{l-1}.$$

Similarly, we can show that for $\mathbf{I}_{\omega,k,t} \in \mathcal{I}_{l-1}$,

$$(\mathbf{I}_{\omega,k,t}) - (l_1 - 1) \in \mathcal{G}_{l_1,l_2}.$$

We can thus define a function $f : \mathcal{G}_{l_1,l_2} \rightarrow \mathcal{I}_{l-1}$ given by:

$$f(\mathbf{G}_{\omega_1,\omega_2,k,t}) = (\mathbf{G}_{\omega_1,\omega_2,k,t}) + (l_1 - 1).$$

We show that f is a one-to-one correspondence with the desired property. By Proposition A.1.1, f is one-to-one. Furthermore, f is onto $\mathcal{I}_{l-1}$ since for $\mathbf{I}_{\omega,k,t} \in \mathcal{I}_{l-1}$, $(\mathbf{I}_{\omega,k,t}) - (l_1 - 1) \in \mathcal{G}_{l_1,l_2}$, and $f((\mathbf{I}_{\omega,k,t}) - (l_1 - 1)) = ((\mathbf{I}_{\omega,k,t}) - (l_1 - 1)) + (l_1 - 1) = \mathbf{I}_{\omega,k,t}$. Finally, for $\mathbf{G}_{\omega_1,\omega_2,k,t} \in \mathcal{G}_{l_1,l_2}$, the cardinality of $f(\mathbf{G}_{\omega_1,\omega_2,k,t})$ is the same as that of $\mathbf{G}_{\omega_1,\omega_2,k,t}$ since for $\mu_1, \mu_2 \in \mathbf{G}_{\omega_1,\omega_2,k,t}$,

$$\mu_1 \neq \mu_2 \Rightarrow \mu_1 + (l_1 - 1) \neq \mu_2 + (l_1 - 1)$$

by Proposition A.1.1. □

Corollary A.1.5 *The general indicial bases* $\mathcal{V}_{n,1,l}$, $\mathcal{V}_{n,2,l-1}$, ..., $\mathcal{V}_{n,l,1}$ *all have the same cardinality.*

We leave it to the reader to extend the results of Section 3.3 using Theorem A.1.4.

Bibliography

[Cip87] Barry A. Cipra. An introduction to the Ising model. *American Mathematical Monthly*, 94:937–959, 1987.

[Fuc89] Norman H. Fuchs. Approximate solutions for large transfer matrix problems. *Journal of Computational Physics*, 83(1):201–211, 1989.

[Gar83] Solomon Gartenhaus. Approximation method for spin-half Ising models. *Physical Review B*, 27(3):1698–1718, 1983.

[Isi25] Ernst Ising. Beitrag zur theorie des ferromagnetismus. *Z. Physik*, 31:253–258, 1925.

[Kac68] Mark Kac. *Mathematical Mechanisms of Phase Transitions*. Gordon and Breach, New York, 1968. Brandeis Lectures.

[KW41] Hendrick A. Kramers and Gregory H. Wannier. Statistics of the two-dimensional ferromagnet, I and II. *Physical Review*, 60:252–262,263–276, 1941.

[Ons44] Lars Onsager. Crystal statistics I. A two-dimensional model with an order-disorder transition. *Physical Review*, 65:117–149, 1944.

[PH91] Beresford N. Parlett and Wee-Liang Heng. The method of minimal representations in 2D Ising model calculations. Technical report, U.C. Berkeley, 1991. In preparation.

[Tho79] Colin J. Thompson. *Mathematical Statistical Mechanics*. Princeton University Press, 1979.

Legal Notice